Journal of Universal Computer Science, vol. 15, no. 15 (2009), 3038-3058
submitted: 1/2/09, accepted: 29/8/09, appeared: 1/9/09 © J.UCS

Managing Security and its Maturity in Small and Medium-sized Enterprises

Luís Enrique Sánchez, Antonio Santos-Olmo Parra
(SICAMAN NT. Departament of R+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
lesanchez@sicaman-nt.com, asolmo@sicaman-nt.com)

David G. Rosado, Mario Piattini
(ALARCOS Research Group. TSI Department. UCLM Research and Development Institute
University of Castilla-La Mancha, Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
David.grosado@uclm.es, Mario.Piattini@uclm.es)

Abstract: Due to the growing dependence of information society on Information and Communication Technologies, the need to protect information is getting more and more important for enterprises. In this context, Information Security Management Systems (ISMSs), have arisen for supporting the processes and systems for effectively managing information security. The fact of having these systems available has become more and more vital for the evolution of Small and Medium-Sized Enterprises (SMEs), but however, this type of enterprises have special characteristics which make it difficult for them the correct deployment of ISMSs. In this article, we show the methodology that we have created for the development, implementation and maintenance of ISMSs, adapted for the needs and resources available for SMEs. This approach is being directly applied to real case studies and thus, we are obtaining a constant improvement in its application.

Keywords: ISMS, SME, Security System
Categories: K.6.5, L.4

1 Introduction

In a global and competitive business environment as the one existing today, enterprises depend more and more on their information systems because it has been proved that they have an enormous influence on improving the level of competitiveness of enterprises [Ashish, Curtis et al. (2003); Cavusoglu, Mishra et al. (2004)]. Nevertheless, without an adequate *security management*, these information systems lack real value since they cannot provide enterprises with enough guarantees of business continuity [Humphrey (2008)]. For that reason, enterprises start being conscious of the huge importance of having adequate information systems as well as a correct management of them. In this way, in spite of the fact that there are still many enterprises assuming the risk of lacking adequate protection measures, there are many others that have understood that information systems are not useful without security management systems and the protection measures associated with them [Doherty and Fulford (2006)].

A great part of this mentality change in enterprises has its origin in the social change produced by the Internet along with the speed of information interchange that

has caused that enterprises become conscious of the value of information for their organizations and worry about protecting their data. This way, enterprises are already conscious of the fact that information and the processes that support systems and nets are their most important assets [Kluge (2008)]. These assets are submitted to a great variety of risks that can critically affect the enterprise. Thus, the importance of security in information systems is supported by numerous works [Masacci, Prest et al. (2005); Walker (2005)], just to mention some of them.

In the past, the enterprises that decided to protect their information systems faced these projects from the perspective of considering that security was individual, in other words, that only affected an object and not the whole set to which the object belonged. That is to say, they were based on the implementation of security measures but without carrying out an adequate management of such measures [Humphrey (2008)]. As time went by, as enterprises did not have an adequate management, the implemented controls were not maintained and were converted into passive controls that instead of helping improve security, contributed to misinforming, offering erroneous information in many cases. Thus, in [Tsujii (2004)], authors highlight the fact that technological aspects are not enough for the construction of a security system but management as well as legal and ethical aspects are necessary too.

In fact, experts consider that security in information systems has a bi-dimensional character [Siponen (2006)]. Today, security in information systems is not dealt with as an exclusively technical aspect where the correct use of certain security mechanisms (e.g. security protocols, cipher schemas, etc) guarantees the security of a system in absolute terms. Besides, and given the social integration of software systems, there is a new dimension that becomes very relevant and must be carefully analyzed. This new dimension has mainly a social and organizational character and is linked to the fact that the interaction between mankind and secure information systems is becoming higher. There are research results that have shown that the human factor has a significant impact on security [Schumacher (2003)].

The problem of information security is characterized by its complexity and interdependence. Security management contains an important number of factors and elements that are interrelated between them. SMEs in developed countries normally have a weak comprehension of information security, security technologies and control measures and so, they tend to forget about risk analysis or the development of security policies [Gupta and Hammond (2005)]. This can be due to the fact that SMEs lack the resources, time and specialized knowledge necessary for coordinating information security or offering adequate information about security, training and education. However, the literature suggests a very different explanation. [Johnson and Koch (2006)] state that SMEs do not want to pay for security and they prefer to maintain a physical security they are familiarized with. Additionally, SMEs do not consider that security is linked to the enterprise strategy and this fact directly impacts on its fulfilment [O'Halloran (2003)]. In fact, a recent research puts forward the need to link information security to strategic planning information systems and therefore, to the enterprise objectives [Doherty and Fulford (2006)].

Despite that there are numerous security standards in Information and Communication Technologies, such as the code of good practice [ISO/IEC27001 (2005)], methodologies for security management such as COBIT [COBITv4.0 (2006)], or for risk analysis and management such as Magerit [MageritV2 (2006)], or

even maturity models for information security management such as SSE–CMM [SSE-CMM (2003)], they are normally designed for big corporations, are very rigid and their practical application in SMEs requires plenty of time and is very expensive. These are the reasons why many enterprises offer resistance to the implementation of adequate security management techniques, thus assuming security risks and so, the loss of competitiveness that are not acceptable in the modern enterprise.

In many bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs [Tuffley, Grove et al. (2004); Wiander and Holappa (2006); Barlette and Vladislav (2008)] is detected and highlighted. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified many times.

In this paper, we will describe the methodology that we have developed for security management in SMEs with the aim of solving the problems detected in the classical methodologies that have shown not to be efficient at the time of their implementation into SMEs due to their complexity and other series of factors that will be analyzed in detail in the following sections of the paper. This methodology allows us to develop, implement and maintain an ISMS using a very reduced number of resources, at a low cost, supporting part of the complexity of its management system over a tool validated in real environments.

The remainder of the paper is structured as follows. In section 2, we will briefly describe the existing methodologies and models for security management and their current tendency. In section 3, we will introduce our proposal of methodology for security management oriented to SMEs. In section 4, we will show the tool developed to support the methodology and some of the major lessons learned during its development and finally in Section 5, we will conclude indicating the work that we will develop in the future.

2 Related Work

With the purpose of reducing the lacks shown in the previous section as well as the losses caused by them, a great number of processes, frameworks and methods of security information whose need of implementation is being more and more recognized and considered by organizations have appeared. However, as it has been shown, they are inefficient for SMEs.

Among them, we can highlight the model presented in the family of standards ISO/IEC27000 [ISO/IEC27000 (2009)], mainly standards ISO/IEC27001 [ISO/IEC27001 (2005)] and ISO/IEC27002 [ISO/IEC27002 (2007)], that of COBIT [COBITv4.0 (2006)] and the information security management maturity model [ISM3 (2007)]. In [Von Solms (2005)] and [Pertier (2003)], authors offer a study of the coexistence and complementary use of COBIT [COBITv4.0 (2006)] and ISO/IEC27002 [ISO/IEC27002 (2007)] through the development of a mapping for the synchronization of both frameworks. Some of the detractors of ISO/IEC27002 [ISO/IEC27002 (2007)] present, as a disadvantage, the fact that it is a support guide but it does not reach all the necessary framework for the government of information technologies. Its main advantage against COBIT [COBITv4.0 (2006)] is that it is

more detailed and has more guides oriented to how things must be done. A recent report of the ITGI (Information Technology Government Institute) solves the problem of synchronization by developing a mapping between COBIT [COBITv4.0 (2006)] and ISO/IEC27002 [ISO/IEC27002 (2007)].

Following this "philosophy", many other more specific maturity models have been proposed: for project management [McBride, Henderson-Sellers et al. (2004)], requirements engineering [Sommerville and Ransom (2005)], distributed development [Ramasubbu, Krihsnan et al. (2005)], maintenance [April, Huffman et al. (2005)], outsourcing [KcKinney (2005)], architectures [NASCIO (2003); Schekkerman (2003); OMB (2004); Van der Raadt, Hoorn et al. (2005)], security [SSE-CMM (2003)], e–Government services [Widdows and Duijnhouwer (2003)], etc.

In many bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs [Tuffley, Grove et al. (2004)] is detected and highlighted. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified many times. Moreover, organizations, even the big ones, tend more to adopt groups of processes related as a set than to deal with processes independently [Mekelburg (2005)].

As we have shown, the methodologies and security management models aforementioned are not valid for SMES due to three reasons:

- They were developed thinking of organizations with more resources available.
- They only deal with part of the security management system and almost none of them focus the implementation of these systems from a global point of view; forcing the enterprises to acquire, implement, manage and maintain several methodologies, models and tools to manage security. Additionally, the few applications that have attempted to deal with all security management aspects are expensive to acquire and require a complex management and a costly maintenance and this fact makes them inadequate for SMEs.
- Finally, we can conclude that, although there are several standards, regulations, guides of good practice, methodologies and models of security management and risk analysis, they are not integrated into a global model that can be applicable to small and medium-sized enterprises with guarantee of success.

Therefore, and as a conclusion of this section, we can state that it is pertinent and appropriate to focus the problem of developing a new methodology for the management of security and its maturity for SMEs information systems with a model that validates its functioning along with a tool that supports the model taking as a basis the problem that this kind of enterprises face and that has lead to continuous failures when attempting the implementation into this kind of enterprises.

3 MMSM-SME: Methodology for ISMS in SMEs

The methodology for the management of security and its maturity in SMEs that we have developed allows any organization to manage, evaluate and measure the security

of its information systems but it is mainly oriented to SMEs because they are the enterprises with a higher rate of failure in the implementation of the existing security management methodologies.

One of the objectives pursued by the MMSM–SME methodology is to be easy to apply and that the model developed with it, allows us to obtain the highest possible level of automation with minimum information, collected in a very short period of time. In the methodology, we have prioritized speed and cost saving and to do so we have sacrificed the precision offered by other methodologies. That is to say, the developed methodology has the purpose of developing one of the best security configurations but not the optimum one, prioritizing time and cost saving against precision although guaranteeing that the obtained results have enough quality.

Other of the main contributions of the methodology is that a matrix set allowing us to relate the different components of the ISMS (controls, assets, threats, vulnerabilities, risk criteria, procedures, registers, templates, technical instructions, regulations and metrics) has been developed. Our methodology will use it to automatically generate a great part of the necessary information, reducing in a notorious way the necessary time for ISMS development and implementation. This set of interrelations between all the ISMS components allow that the change of any of these objects alters the measurement value of the rest of objects composing the model in a way that, at any time, we can have an updated valuation of how the security system of the enterprise evolves.

We have developed our methodology of management and maturity of information system security and a model associated with it, through the action-research method [Kock (2004)], and taking into account the feedback obtained from their application to actual case studies with our clients.

This methodology is composed of three main subprocesses:

- GEGS. Generation of Security Management Schemas: The main purpose of this subprocess is the construction of "schemas", that are structures necessary for the ISMS construction, created for a set of enterprises that share similar characteristics. These schemas are reusable and allow us to reduce the time of creation of the ISMS as well as its maintenance cost; thus becoming adequate for SMEs dimension. The use of schemas is especially interesting and relevant in the case of SMEs because, due to their special characteristics, they normally have simple and very similar information systems.
- GSGS – Generation of Security Management Systems. The main goal of this subprocess is the creation of an ISMS appropriate for the enterprise using, to do so, an existing schema.
- MSGS – Maintenance of the Security Management System. The main objective of this subprocess is to maintain and manage the security of the information system of the enterprise, providing updated information at the time of a generated ISMS.

3.1 Previous definitions

To facilitate the understanding of the methodology, a set of frequently used concepts in our methodology are described below:

- **Schema:** Structure formed by the main elements of an ISMS and the relations between them that can be reused by a set of enterprises with common

characteristics (same sector and size) from the knowledge acquired with the implementation of the MGSM-PYME methodology and further refinements.
    - **Base Schema:** Initial schema obtained from the knowledge of security experts that serves as a basis for the elaboration of other more specific schemas that can be adequate for a set of enterprises.
- **ISMS:** Part of a global management system that, based on risk analysis, establishes, implements, operates, monitors, reviews, maintains and improves information security [ISO/IEC27001 (2005)]. In the case of MGSM–PYME methodology, the ISMS is composed of, among others, a set of regulations that define the security policy of the enterprise, procedures, controls, a simple risk analysis and a balanced scorecard that allows us to know how the system evolves.
- **Maturity Level:** Measure that attempts to establish a standardized valuation with which we can determine the state of security information within an organization and the way to reach the adequate security level in that enterprise.
- **Control:** Policies, procedures, practices and organizational structures created to maintain the risks of security information below the assumed risk level.
- **Role/Profile:** Position or responsibility of a user within the organization chart of an enterprise. In MGSM–PYME methodology, all users have one or several roles associated.
- **Regulations:** Set of rules conforming the policy of security management of the ISMS.
    - **Rule** Norm of behaviour that must be fulfilled because it has been decided collectively and whose unfulfillment will carry out a penalty.
- **Risk analysis:** Systematic process for estimating the size of the risks to which an organization is exposed [MageritV2 (2006)]. The MGSM–PYME methodology includes a simple method to estimate the risk from a basic set of assets.
    - **Asset:** Resources of the information system or related to it that the enterprise needs to work correctly and to achieve the objectives proposed by the managing board. [MageritV2 (2006)].
    - **Threat:** Event that can cause an incident in the organization, causing material damages or immaterial losses in the assets [MageritV2 (2006)].
    - **Vulnerability:** -Weakness or lack of control that would allow or facilitate that a threat acts against an asset of the system presenting such weakness [MageritV2 (2006)].
    - **Risk criteria:** Criteria that allows us to estimate the degree of exposure to which a threat can become true over one or more assets causing damages or prejudices to the organization.
- **Procedure:** It defines the sequence in which the methods, the required deliverables (registers, templates, etc), the controls that help us assure the information system and the norms that help us manage it are applied. In MGSM–PYME methodology, the procedures are formed by a set of phases of different types.
    - **Phase:** Part of a process or procedure with a specific function. In MGSM–PYME methodology, each phase has associated: i) one or

several roles that define which users can execute that phase; ii) one or several phases to which we can go from the current phase; called paths; y iii) a set of objects (templates, registers and technical instructions) that will be used during the phase.
    - **Template:** Document that provides us with a separation between the form or structure and the content.
    - **Register:** Type of structured document formed by the union of several elements under a same structure.
    - **Technical instruction:** Technical support documents.
- **Security culture:** Set of properties that help both individuals and the organization as a whole act with higher effectiveness and efficiency improving the security management of the information system.
    - **Certificate of security culture:** Document that shows that a user has achieved the desired level of security culture.
- **Balanced Scorecard:** Visual system that collects the main security indicators presenting the information considered essential in a simple and of course.
- **The balanced scorecard** is a system that informs us of the evolution of the main security parameters. In MGSM–PYME methodology, the main objective of the balanced scorecard is that of allowing us to follow at all times the security level of the controls composing the ISMS.
    - **Metric:** Measure to know or estimate the characteristics that affected an information system (for example, level of fulfillment of the security controls, response time to an incident etc).
- **Information Repository:** Centralized place where data and data structures are stored. MGSM–PYME methodology is composed of three main repositories:
    - **Schemas Repository:** Warehouse where the different components of the schemas generated in the GEGS process will be stored.
    - **ISMS Repository:** Warehouse where the different components of the ISMS generated by the enterprises will be stored.
    - **ISMS Information Repository:** Warehouse where the results and statistics obtained from the daily use by the ISMS's users will be stored.

3.2 Objectives

The main objectives of our methodology, considered essential for its success, are the following:

- **Reduced number of levels:** Due to the basic structure of SMEs, they are more receptive to three-level maturity models than to the five-level maturity models of the classical systems.
- **Certification by levels:** SMEs are more receptive to the possibility of obtaining an acknowledgement when achieving a level in a short period of time than to the need to readapt all their security system to be able to obtain such acknowledgement.
- **Cost Reduction:** SMEs require that the implementation and maintenance of a ISMS has a very low cost.
- **ISMS time reduction:** The period of development and implementation of the ISMS will be short to adapt itself to the changing structure of SMEs.

- **Improvement in the success percentage of implementations:** To reduce the failure rate in the ISMS implementation using the resources appropriate for the type of enterprise.
- **Evolutive security Management Systems:** Security must be implemented in an evolutive way obtaining short-term results that show the effectiveness of the process. The developed methodology coincides with the appreciations of [Eloff and Eloff (2003)] in which they suggest to carry out a progressive implementation of the controls that allows the enterprise to adapt itself to the security evolution in a non traumatic way.
- **Reuse:** Obtain data structures that allow us to save part of the ISMS generation cost in enterprises sharing common characteristics.
- **Minimize the maintenance and information collection costs:** The information will be automatically generated according to basic information.
- **Prioritize costs against precision:** Cost saving will be prioritized against precision looking for a security configuration with enough quality, but not the optimum one and always prioritizing time and cost saving.
- **Dynamic evolution of the security level:** Ability to recalculate the current security level with the lowest cost.
- **Versatility:** The methodology is dynamic and adaptable to the specific characteristics of the enterprises.
- **Minimize the use and management of documents:** The methodology must allow us to carry out a double function in the management of the documents associated with security. On the one hand, as contents manager and on the other hand, automatizing and managing the information of the contents to make their fulfillment more dynamic and benefit as much as possible from the information that we can extract from the contained data.
- **Basic risk Analysis**: The risk analysis must have a very reduced generation and maintenance cost; even sacrifying its precision but always maintaining its results with enough quality**.**
- **Automatization:** It must have a tool that allows us to automate the management of the processes composing the methodology.

With the developed methodology, we have reached these objectives necessary for the success of the methodology in SMEs.

3.3 Actors

In this section, we show the set of actors involved in the different subprocesses defined in MGSM–PYME. In practice, many of the roles of these actors will be played by a same individual, because SMEs staff is normally very limited. These actors are the following:

- Client (Cl): It will be the organization that will receive the information security management system. Within the client actor, there are a series of clearly-defined profiles. i) Cl/RS – Responsible for security; ii) Cl/US – Information System Users; iii) Cl/GDS – System Department Manager; iv) Cl/PS – Services Provider; v) Cl/PA – Assets Owner; vi) Cl/GD – Department Manager; vii) Cl/RD – Responsible for Development; vii) Cl/RE – Responsible for Exploitation; viii) Cl/RM – Responsible for Marketing; ix) Cl/RR – Responsible for Human Resources; and x) Cl/T – Third Parties.

- **Security Management Architect (AGS)**. The main responsibilities of this actor will be:
    - Analysis of the information obtained from the balanced scorecard of the implemented ISMS.
    - Configuration and recalibration of the schemas defined for each enterprise.
    - Proposals of improvement for the audits carried out from the information obtained from the case studies.
    - Reusability in such a way that the security management methodology is reusable for future projects.
- **Group of Experts in the Domain (GED):** It represents the individual or set of individuals who know the Domain of the problem to deal with.
- **Security Consultant (CoS):** He/She will work together with the speaker designed by the client for the achievement of the information necessary for the generation of the structure of the ISMS of the enterprise.
- **Speaker (Int):** He/She will be an employee of the enterprise where the ISMS will be implemented, designed by the client (CI) to work together with the security consultant (CoS) acting as an intermediary between the security consultant and the enterprise. Additionally, he/she will be the responsible for approving the final result obtained from the application of the methodology. The functions of the speaker will be normally performed by the responsible for security (Cl/RS).
- **Security Auditor (AuS):** He/she will work together with the responsible for security (Cl/RS) and the rest of client profiles to verify that the defined structure for security management covers the security requirements, thus providing an external validation to the organization. Furthermore, he/she will verify that the security controls are the correct ones and the security procedures are well specified.

3.4 GEGS – Generation of Security Management Schemas.

Generation of Security Management Schemas (GEGS), is the first subprocess of the MMSM–SME methodology and its main objective is to produce a schema containing all the structures necessary for generating an ISMS and those relations that could be established between them for a determined type of enterprises (same sector and size) with the aim of saving time and resources at the time of generating an ISMS for an enterprise that has the same characteristics as those for which the schema was created.

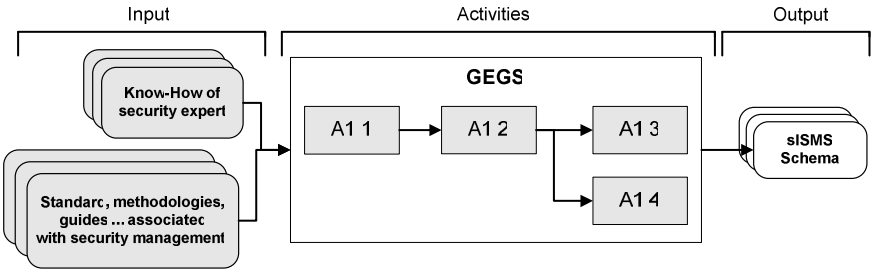

Figure 1: Simplified schema at activity level of GECS subprocess

In [Fig. 1] we can see the basic schema of inputs, activities and outputs composing this subprocess:

- **Inputs:** As input, we will receive the knowledge of the Group of Experts in the security Domain (GED) obtained during the process of ISMS implementation. This knowledge is recurrent and incremental during the whole lifecycle of the methodology. The second input will be formed by a set of elements coming from regulations, guides of good practice and other existing methodologies that will be used along with a schema for ISMS construction.
    - The knowledge of the experts that has been acquired during other ISMS implementations (for example, relations between elements, procedures, etc).
    - Lists of elements coming from other regulations, guides of good practice (such as ISO/IEC27002) or methodologies (such as Magerit v2).
- **Activities:** The subprocess is composed of four activities. Activity A1.2 could not be carried out until Activity A1.1 is finished because it requires elements generated by this activity for its correct functioning. Activity A1.3 and A1.4 depend on elements generated by A1.2 and therefore, they will have to wait for its finalization. Between activities A1.3 and A1.4, there are no time dependencies and so, they can be executed in a parallel way. In [Fig. 2], we can see in detail the different objects composing the schema.
    - A1.1 – Generation of master tables: The initial configuration tables are established and they will contain: i) the roles of the information system users that will be able to participate in the system; ii) the different business sectors to which the enterprise can belong; and iii) the maturity levels over which the ISMS could evolve throughout its lifecycle.
    - A1.2 – Generation of maturity level tables: We will select maturity rules that will allow us to determine the current maturity level of the ISMS of the enterprise and the list of controls that could be established. These controls will be divided into subcontrols to be able to find out the approximate level at which they are currently fulfilled with higher precision. Also, these subcontrols will be associated with the maturity levels defined in the previous activity.
    - A1.3 – Generation of risk analysis tables: We select the list of elements of the artefacts associated with risk analysis as well as the relations existing between them.
    - A1.4 – Generation of tables of the artefacts library: We select the list of elements of the artefacts associated with the ISMS generation along with the relations existing between them.

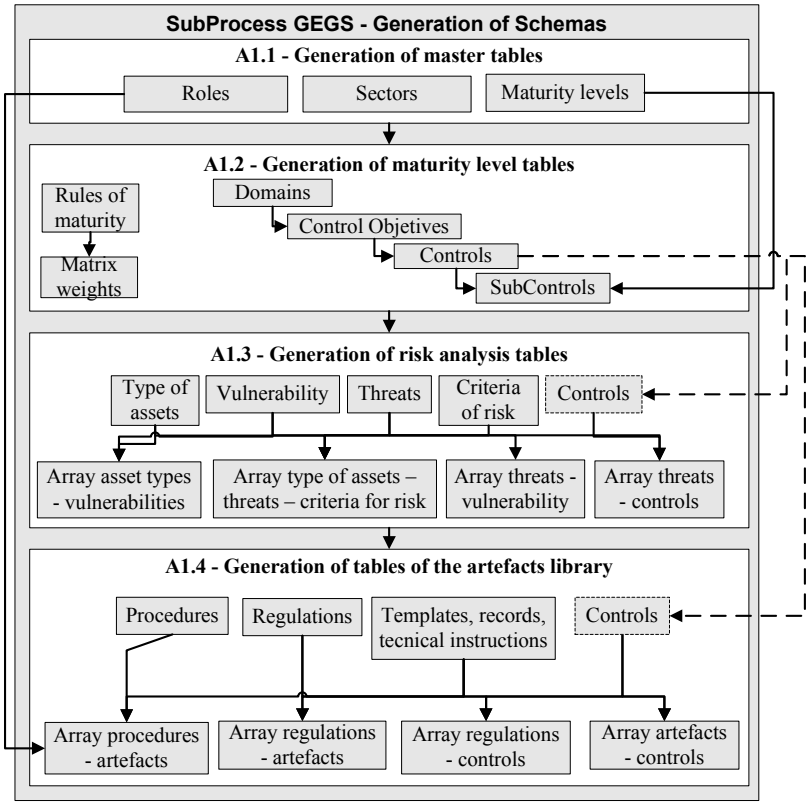

Figure 2: Elements of GEGS subprocess.

- **Outputs:** The output produced by this subprocess will consist of a complete schema formed by all the necessary elements to build an ISMS and the existing relationships between these elements.
    - A subset of elements selected from the input lists.
    - A matrix series that relate the main elements (controls, types of assets, vulnerabilities, threats and risk criteria) necessary for the elaboration of a risk analysis between them.
    - A matrix series that relate the main elements (controls, procedures, regulations, templates, registers, technical instructions) necessary for the ISMS generation between them.

All this set of artefacts necessary for generating the management system of the enterprise information system are included in the repository of schemas for ISMS that is constantly updated with the new knowledge obtained in each new implementation.

Due to the complexity of the development of a schema and as part of the research, we have developed an initial schema called base schema (EB), obtained from the knowledge acquired during the research process, with the purpose of making it possible the creation of new schemas through a cloning process (generate a new

schema from an existing schema) of the base schema and after that, performing the necessary adjustments in the new schema to adequate it to the desired type of enterprises.

It is important to highlight that this process will only have to be carried out when at the time of performing an ISMS implementation, we do not have in the repository any schema appropriate for the type of enterprise (size and sector) for which we are aimed at creating the ISMS.

3.5 GSGS – Generation of the Security Management System.

The Generation of the Security Management System (GSGS) is the second subprocess and its main objectives are on the one hand, the ISMS generation through the selection of the most adequate schema for the type of enterprise and on the other hand, the request of business and technical information of the enterprise performed by a speaker (Int) designed by the enterprise.

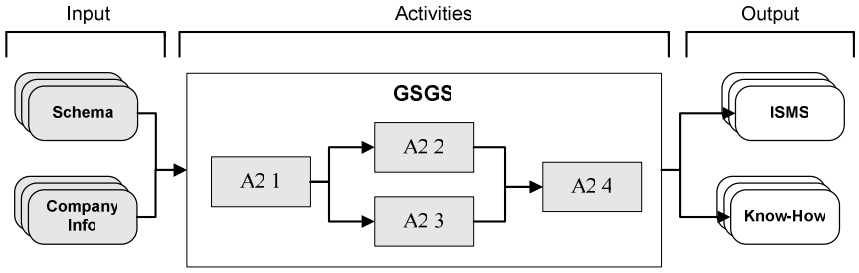

Figure 3: Simplified schema at activity level of GSGS subprocess

In [Fig. 3], we can see the basic schema of inputs, activities and outputs composing this subprocess.

- **Inputs:** As inputs, we will receive a schema taken from those existing in the repository of schemas that is appropriate for the characteristics of the enterprise over which we are aimed at generating the ISMS, as well as technical and business information of the enterprise.
    - Information of the enterprise in which we want to carry out the ISMS: i) business information; ii) valid speaker for the development of the ISMS; iii) enterprise organization chart; and iv) list of users and the roles that they perform within the information system of the enterprise.
    - The most adequate schema to generate the ISMS from the business profile of the enterprise and from the repository of schemas.
    - Two lists of verification: i) a list of verification with business information; ii) a list of verification with information about the level of security management.
    - A list of assets associated with the information system of the enterprise, trying to group them into the lowest possible number of assets (thick grain) to reduce the cost of the generation and management of the information system.

- **Activities:** The subprocess will be formed by four activities. Activities A2.2 and A2.3 could not be carried out until activity A2.1 is finished because they require elements generated by this activity for their correct functioning. Activity A2.4 depends on elements generated by activities A2.2 and A2.3 so it will have to wait for the finalization of them. In [Fig. 4], we can see the different objects composing this subprocess.

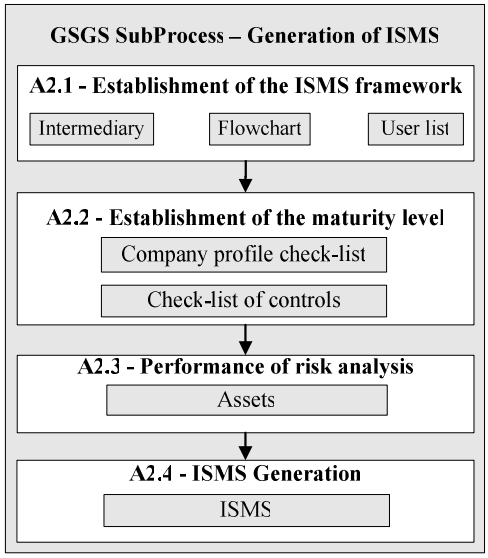

Figure 4: Elements of GSGS subprocess.

- A2.1 – Establishment of the ISMS framework: We will establish the relations with the enterprise, defining a valid speaker and requesting information from the enterprise: i) enterprise organization chart; ii) users with access to the information system and roles represented by them.
- A2.2 – Establishment of the maturity level: i) Through a business meeting, we request information related to the enterprise (number of employees, turnover, etc) with the objective of determining the most adequate schema for this type of enterprise among those existing in the repository of schemas; and ii) A second meeting, this one of a technical character, is carried out to determine in detail the current situation of the enterprise with respect to the security management of its information system.
- A2.3 – Performance of risk analysis: A set of basic assets of thick grain, will be identified determining the cost (qualitative and quantitative) that their loss would mean for the organization. From the set of assets, we will determine the security risks to which they are submitted and a plan to mitigate them in an efficient way will be generated.

  - A2.4 – ISMS Generation: From the obtained information and the selected schema, the elements that will form the ISMS for the enterprise will be generated and we will proceed to implement it into the enterprise.

- **Outputs:** The output produced by this subprocess will consist of a set of elements selected from the schema and from the introduced information as well as a set of reports with information about the current state of the enterprise and the measures that will have to be taken to improve the security management level.
  - The current maturity level of the enterprise with respect to its information security management system and to what maturity level it should progress.
  - A matrix with the risks to which the assets of the enterprise are submitted.
  - An ordered improvement plan that indicates which controls should be reinforced for the security level of the enterprise to evolve as fast as possible.
  - A set of elements that compose the ISMS of the enterprise including: i) a control board that indicates the security level for each control related to security management; ii) a set of regulations, templates and technical instructions valid for this enterprise in the current moment; iii) a set of metrics; iv) a set of users, associated with roles that will allow us to execute a series of procedures to interact with the information system; and v) a set of regulations that must be fulfilled for the ISMS functioning.

All this set of objects that compose the ISMS are included in the ISMS repository and will be used by the enterprise to be able to correctly manage the security of the information system.

3.6 MSGS – Maintenance of the Security Management System.

The maintenance of the Security Management System (MSGS) is the third subprocess defined in MMSM–SME and its main purpose is to allow the performance of the set of tasks necessary for being able to work with the ISMS, to measure its evolution and to facilitate the collection of knowledge for the continuous improvement of the generated schemas and ISMSs.

In [Fig. 5], we can see the basic schema of inputs, activities and outputs composing this subprocess:

- **Inputs:** As inputs, we will receive a set of elements (regulations, procedures, controls and their current level of fulfillment) generated during activity A2.4 and that compose the ISMS.
  - A set of users and the roles that they will develop within the information system; these roles will determine which procedures they have access to.
  - A set of regulations that must be fulfilled for the good functioning of the ISMS.

- A set of security procedures and the elements (templates, registers, technical instructions) associated with them.
- A control board that will indicate the security level for each control related to the security management of the enterprise.

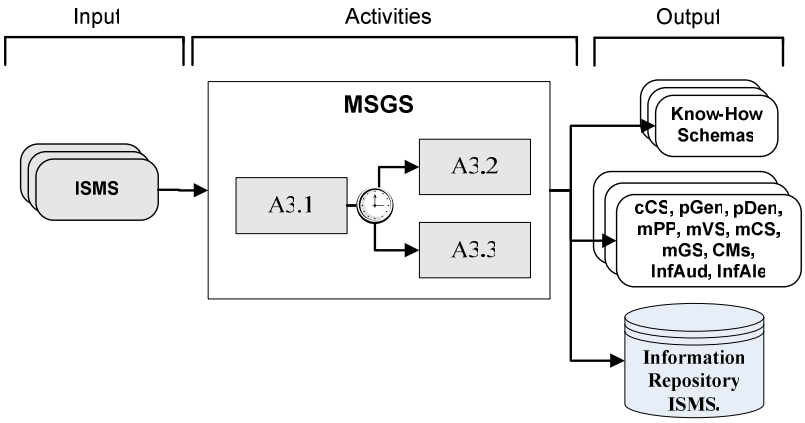

Figure 5: Simplified schema at activity level of MSGS subprocess

- **Activities:** The MSGS subprocess for ISMS maintenance is basically composed of the following activities. Activities A3.2 and A3.3 will always require that activity A3.1 had been carried out first to be executed and they could be executed as many times as necessary during the lifecycle (represented by a clock in the schema). In Figure 6, we can see the different objects composing this subprocess.
  - A3.1 – Obtain or renew the certificate of security culture: We will establish a system that allows creating in a progressive way a security conscience among the users of the information system that guarantees its quality.
  - A3.2 – Execute ISMS procedures: General and specific (for example, complaint procedure) that will allow the ISMS of the enterprise to be updated will be executed.
  - A3.3 – Follow-up of the ISMS fulfilment. We will have a set of metrics to keep the control board of the security of the enterprise updated in a dynamic way and in real time for the responsible for security to be able to make decisions without waiting for the performance of an external audit.

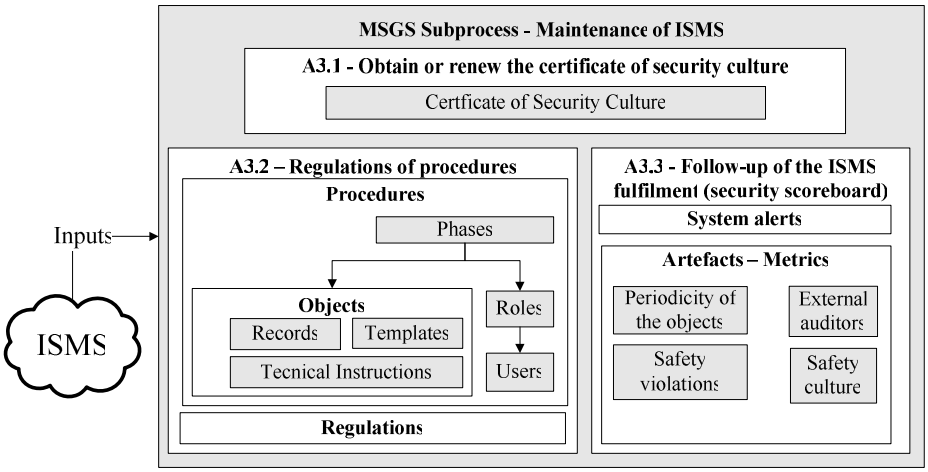

Figure 6: Elements of MSGS subprocess

- **Outputs:** The output produced by this subprocess will consist of:
  - A series of instances of the existing procedures that will be executed as time goes by and that will allow us to manage and maintain the ISMS of the enterprise.
  - A set of metrics that will allow us to maintain the control board associated with the security level of the ISMS updated: i) a set of general metrics; ii) specific metrics: regular recurrence of objects, security violations, security conscience and external audits.
  - Statistics extracted from the daily use of the ISMS carried out by the users of the information system that will be converted into knowledge for experts in security to be able to elaborate new schemas and refine those already existing.

All output information generated during the useful lifecycle of the ISMS will be included in the repository of information of the ISMS and will be used by the enterprise to be able to correctly manage information system security as well as by the group of experts in security to improve the schemas of GECS subprocess.

4 Applicability of MMSM-SME

To validate the MMSM-SME methodology, a tool called MMSM-TOOL has been developed. This tool allows us to develop simple, inexpensive, fast, automated, progressive and sustainable security management models. These are the main requirements that this type of enterprises have at the time of implementing these models.

From the viewpoint of the user, this tool presents two clear advantages:

- Simplicity: All ISMS activities are oriented to reduce the complexity of the process of construction and maintenance of ISMSs, thinking of organizations (SMEs) whose organizational structures are very simple.
- Automation: The whole system uses a concept called schemas to be able to automate the necessary steps to build and maintain the ISMS of the enterprise.

The tool is composed of three clearly differentiated parts and that correspond to the subprocesses of the methodology:

- Schemas Generator (GEGS): This zone of the tool can only be accessed by the security management architect (AGS) and the group of experts in the Domain (GED) and from this zone, we can carry out three basic operations: i) create new schemas; ii) clone schemas from an existing schema; and iii) modify schemas to improve the ISMS generation.
- ISMS Generator (GSGS): This zone of the tool can only be accessed by the security consultant (CoS) and the objective here is that of generating the ISMS for the enterprise.
- ISMS Support del ISMS (MSGS): This zone of the tool can be accessed by the users of the information system. The most relevant profile within this zone is the responsible for security (RS). From this zone, we can carry out three basic operations: i) management of the certificates of security culture; ii) procedure management; and iii) control board management.

Schemas are the nucleus over which the tool is developed because they allow the ISMS automation. These schemas are formed by a set of elements and associations between them, defined from the knowledge acquired by the customers.

The tool has allowed us to reduce the implementation costs of the systems and implies a higher percentage of success in implementations into SMEs. For these reasons, we consider that the results of this research can be very positive for SMEs because this tool allows them to access to the use of security management with a cost of resources reasonable for their size. Also, through the use of this methodology and the tool supporting it, we can obtain short-term results and reduce the costs that the use of other models and tools implies, thus obtaining a higher degree of satisfaction and efficiency in the enterprise.

Additionally, the tool allows us to maintain repositories containing not only information about the specifications of the necessary schemas for the construction of ISMSs but also information about the results obtained in the different use cases, thus allowing the constant improvement of the methodology along with the models.

From the application of the methodology and its tool to practical cases, we have extracted some interesting data:

- Information system users are not reluctant to security when its application is simple and the required knowledge is minimum.
- In the case of SMEs, it is better to obtain less precise data (although keeping enough quality) if with this we obtain huge cost reductions.
- The security culture is fundamental for the success of ISMSs in SMES at long term.

- The short-term knowledge of the level of fulfilment of the involved security controls is fundamental to maintain the ISMS.

5 Conclusions

In this paper, we have presented the proposal of a new methodology for the management of security and its maturity in SMEs. This methodology lets SMEs develop and maintain an ISMS with a cost of resources acceptable for this type of enterprises. In addition, it obtains huge management cost saving and improves the percentage of success in the implementation and maintenance of the ISMS, obtaining progressive improvements of the security culture of the staff of the enterprise involved in its information system.

With the purpose of showing the validity of the methodology, we have defined a model (base schema) that allows supporting the results generated through the research and that fulfils the pursued objectives.

We have defined how this methodology must be used and the improvements that it offers with respect to other methodologies that face the problem partially or in an excessively expensive way for SMEs.

The characteristics offered by the new methodology and its orientation to SMEs has been very well received and its application is showing to be very positive because it allows this kind of enterprises to access to the use of information security management systems and so far, this had only been possible for big enterprises. In addition, with this methodology, we obtain short-term results and we reduce the costs that the use of other methodologies implies, obtaining a higher degree of satisfaction of the enterprise.

At last, we consider that the work done must be widened with new specifications, new schemas, increasing the set of artefacts of the library and deeping into the model with new example cases.

Among the improvements of the model on which we are working as future research lines we can highlight:

- Improvements associated with GEGS subprocess: Adaptation of the predefined schemas for SMEs to the new rules and standards that arise associated with security management.
- Improvements associated with GSGS subprocess: Review aspects related to ISMS generation.
- Improvements associated with MSGS subprocess: Improve and increase the mechanisms of security measurement and auto-evaluation through the introduction of new metrics in the model that allow us to know the security level at any time; thus minimizing the number of auto adjustment audits necessary for maintaining such security level updated.

All these future improvements of the methodology as well as the model are being oriented to improve the precision of the model but always respecting the principle of cost of resources; in other words, we are aimed at improving the model without generating ISMS generation costs and maintenance costs.

Through the "action research" method and with the help of the feedback directly obtained from our customers, we hope to achieve a continuous improvement of these implementations.

Acknowledgements

This research is part of the following projects: BUSINESS (PET2008-0136) granted by the "Ministerio de Ciencia e Innovación" (Spain), QUASIMODO (PAC08-0157-0668) and SISTEMAS (PII2I09-0150-3135), projects financed by FEDER and the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", and MEDUSAS (IDI-20090557) project financed by the "Centro para el Desarrollo Tecnológico Industrial - Ministerio de Ciencia e Innovación"(CDTI).

References

[April, A., J. Huffman, et al. (2005)] April, A., J. Huffman, et al.: "Software Maintenance Maturity Model: the software maintenance process model. Journal of Software Maintenance and Evolution." *Research and Practice* (2005), **17**: 197-223.

[Ashish, G., J. Curtis, et al. (2003)] Ashish, G., J. Curtis, et al.: "Quantifying the financial impact of IT security breaches." *Information Management & Computer Security* (2003), **11**(2): 74-83.

[Barlette, Y. and V. Vladislav (2008)] Barlette, Y. and V. Vladislav: *Exploring the Suitability of IS Security Management Standards for SMEs*. Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, Waikoloa, HI, USA. (2008).

[Cavusoglu, H., B. Mishra, et al. (2004)] Cavusoglu, H., B. Mishra, et al.: "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* (2004), **9**: 69-104.

[COBITv4.0 (2006)] COBITv4.0: Cobit Guidelines, Information Security Audit and Control Association. (2006).

[Doherty, N. F. and H. Fulford (2006)] Doherty, N. F. and H. Fulford: "Aligning the Information Security Policy with the Strategic Information Systems Plan." *Computers & Security* (2006), **25**(2): 55-63.

[Eloff, J. and M. Eloff (2003)] Eloff, J. and M. Eloff: "Information Security Management - A New Paradigm." *Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03* (2003): 130-136.

[Gupta, A. and R. Hammond (2005)] Gupta, A. and R. Hammond: "Information systems security issues and decisions for small businesses." *Information Management & Computer Security* (2005), **13**(4): 297-310.

[Humphrey, E. (2008)] Humphrey, E.: *Information security management standards: Compliance, governance and risk management.* Information Security Tech. Report. (2008).

[ISM3 (2007)] ISM3: Information security management matury model (ISM3 v.2.0), ISM3 Consortium. (2007).

[ISO/IEC27000 (2009)] ISO/IEC27000: ISO/IEC FDIS 27000, Information Technology - Security Techniques - Information security management systems. (2009).

[ISO/IEC27001 (2005)] ISO/IEC27001: ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements. (2005).

[ISO/IEC27002 (2007)] ISO/IEC27002: ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management. (2007).

[Johnson, D. W. and H. Koch (2006)] Johnson, D. W. and H. Koch: *Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?* 39th Annual Hawaii International Conference on System Sciences (HICSS'06). (2006).

[KcKinney, C. (2005)] KcKinney, C.: "Capability Maturity Model and Outsourcing: A Case for Sourcing Risk Management." *Information Systems Control* (2005), **5**.

[Kluge, D. (2008)] Kluge, D.: *Formal Information Security Standards in German Medium Enterprises.* CONISAR: The Conference on Information Systems Applied Research. (2008).

[Kock, N. (2004)] Kock, N.: The threee threats of action research: a discussion of methodological antidotes in the context of an information systems study. *Decision Support Systems*. (2004), **37:** 265-286.

[MageritV2 (2006)] MageritV2: Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2), Ministerio de Administraciones Públicas (Spain). (2006), **326-06-044-8**.

[Masacci, F., M. Prest, et al. (2005)] Masacci, F., M. Prest, et al.: "Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation." *Computer Standards & Interfaces* (2005), **27**: 445-455.

[McBride, T., B. Henderson-Sellers, et al. (2004)] McBride, T., B. Henderson-Sellers, et al.: *Project Management Capability Levels: An Empirical Study*. 11th Asia-Pacific Software Engineering Conference (APSEC´04), IEEE Computer Society. (2004).

[Mekelburg, D. (2005)] Mekelburg, D.: "Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes." *Software Quality Professional* (2005), **7**(3): 4-13.

[NASCIO (2003)] NASCIO: National Association of State Chief Financial Officers. Enterprise Architecture Maturity Model, Version 1.3. National Association of State Chief Financial Officers. Lexington KY. (2003).

[O'Halloran, J. (2003)] O'Halloran, J.: "ICT business management for SMEs." *Computer Weekly* (2003), **December 11**.

[OMB (2004)] OMB: OMB Enterprise Architecture Assessment v 1.0. The Office of Management and Budget, The Executive Office of the President. (2004).

[Pertier, T. R. (2003)] Pertier, T. R.: "Preparing for ISO 17799." *Security Management Practices* (2003), **jan/feb**: 21-28.

[Ramasubbu, N., M. S. Krihsnan, et al. (2005)] Ramasubbu, N., M. S. Krihsnan, et al.: "Leveraging Global Resources: A Process Maturity Framework for Managing Distributed Development." *IEEE Software* (2005): 80-86.

[Schekkerman, J. (2003)] Schekkerman, J.: Extended Enterprise Architecture Maturity Model. Institute for Enterprise Architecture Developments (IFEAD). Amersfoort, The Netherlands. (2003).

[Schumacher, M. (2003)] Schumacher, M.: *Security Engineering with Patterns*, Springer-Verlag.

[Siponen, M. T. (2006)] Siponen, M. T.: Information Security Standards Focus on the Existence of Process, Not Its Content? C. o. t. ACM. (2006), **49:** 97-100.

[Sommerville, I. and J. Ransom (2005)] Sommerville, I. and J. Ransom: "An Empirical Study of Industrial Requirements Engineering Process Assessment and Improvement." *ACM Transactions on Software Engieering and Methodology* (2005), **14**(1): 85-117.

[SSE-CMM (2003)] SSE-CMM: Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326. (2003).

[Tsujii, S. (2004)] Tsujii, S.: *Paradigm of Information Security as Interdisciplinary Comprehensive Science*. International Conference on Cyberworlds (CW'04), IEEE Computer Society. (2004).

[Tuffley, A., B. Grove, et al. (2004)] Tuffley, A., B. Grove, et al.: "SPICE For Small Organisations." *Software Process Improvement and Practice* (2004), **9**: 23-31.

[Van der Raadt, B., J. F. Hoorn, et al. (2005)] Van der Raadt, B., J. F. Hoorn, et al.: *Alignment and Maturity are siblings in architecture assesment*. Caise 2005. (2005).

[Von Solms, B. (2005)] Von Solms, B.: "Information Security governance: COBIT or ISO 17799 or both?" *Computers & Security*. (2005), **24**: 99-104.

[Walker, E. (2005)] Walker, E.: "Software Development Security: A Risk Management Perspective." *The DoD Software Tech. Secure Software Engineering* (2005), **8**(2): 15-18.

[Wiander, T. and J. Holappa (2006)] Wiander, T. and J. Holappa: Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method. *Technical Report*. V. T. R. C. o. Finland. (2006).

[Widdows, C. and F. Duijnhouwer (2003)] Widdows, C. and F. Duijnhouwer: Open Source Maturity Model. Cap Gemini Ernst & Young. New York NY. (2003).