Desirable Characteristics for an ISMS Oriented to SMEs

Antonio Santos-Olmo[1], Luis Enrique Sánchez [1], Eduardo Fernández-Medina[2] and Mario Piattini[3]

[1]SICAMAN Nuevas Tecnologías. Departament R+D
Ave Maria, 5. Tomelloso, Ciudad Real, Spain

[2]GSyA Research Group. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071, Ciudad Real, Spain

[3]ALARCOS Research Group. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071, Ciudad Real, Spain

Abstract. Information Society depends more and more on Information Security Management Systems (ISMSs) and the availability of these systems has become vital for SMEs' evolution. However, this kind of companies need that ISMSs are adapted to their special characteristics as well as optimized from the viewpoint of the necessary resources to implement and maintain them. In this paper, we present an analysis of the different proposals that are arising oriented to implement ISMSs into SMEs with the purpose of determining the characteristics that a security management methodology oriented to SMEs should have.

1 Introduction

It is very important for enterprises to implement security controls that let them know and control the risks they can be submitted to[1, 2], given that the implementation of these controls carries out important improvements for these companies [3].But the implementation of these controls is not enough and enterprises need to use systems that manage security throughout the time, allowing them to react agilely to new risks, vulnerabilities, threats, etc. [4, 5]. However, it is common that enterprises do not have security management systems and if they have them, they are made without adequate guides, without documentation or with insufficient resources [6].

As we will show later in this paper, some proposals for information security management already exist (ISO/IEC27001, ISO/IEC21827, ISM3, Areiza's proposal, Eloff's proposal, ASD, IS2ME, Carey-Smith's proposal, Tawileh's proposal, etc); almost all of them made by international organizations for standardization. Nevertheless, although these proposals are very complete and interesting; they are mainly oriented to big enterprises. In fact, there are numerous research sources ([4, 7]) that confirm that these proposals are not adequate for SMEs at all because they offer processes excessively bureaucratic and expensive for them.

Therefore, considering that SMEs represent the great majority of enterprises at both the domestic and the international level and are very important for the business sector of any country, we believe that going further in the research to improve securi-

Santos-Olmo A., Enrique Sánchez L., Fernández-Medina E. and Piattini M..
Desirable Characteristics for an ISMS Oriented to SMEs.
DOI: 10.5220/0003593801510158
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 151-158
ISBN: 978-989-8425-61-4

ty management for this kind of enterprises can generate important contributions. This can help improve not only SMEs' security but also their level of competitiveness. For this reason, in the last years, we have created a methodology (MMSM-SME) for security management and the establishment of the maturity level of SMEs' information systems [8-10]. In addition, we have built a tool to fully automatize the methodology [11], and we have applied it to actual cases [12]. This has allowed us to validate the methodology as well as the tool.

The paper continues in Section 2, describing the existing methodologies and models for security management and their current tendency in the case of SMEs. In Section 3, we analyze the characteristics that the new methodology should have to be adapted to SMEs. These characteristics have been obtained through the application of the "action-research" method to actual cases. In section 4, the activities composing the new methodology and their main characteristics are introduced. At last, in Section 5, we conclude by indicating the work we will develop in the future.

2 Developed 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 information security methods, whose need of implementation is being more and more acknowledged and considered by organizations, have appeared. However, as shown before, they are inefficient in the case of SMEs.

Regarding the most outstanding standards, we have been able to prove that the majority of security management models have been based on ISO/IEC17799 and ISO/IEC27002 international standards and that the most successful security management models in big enterprises are ISO/IEC27001, COBIT and ISM3 but they are very difficult to implement and demand a too high investment that the majority of SMEs cannot make [13]. Although new very interesting proposals oriented to this kind of companies are arising, they face problems in a very incomplete way.

Among the main security management standards we can find:

- ISO/IEC27001 [14]: This standard was tailored to provide a model for the establishment, implementation, operation, monitoring, review, maintenance and improvement of ISMS. ISO/IEC27001 gives total freedom to decide the criteria to establish the security global process and choose the method to analyze, evaluate and manage risks.
- ISO/IEC20000 [15] and ITIL [16]: They consist of a wide set of management procedures created to make it easier for organizations to achieve quality and efficiency in IT operations.
- COBIT [17]: COBIT is a methodology for the adequate control of technology projects, information flows and the risks that the lack of adequate controls implies.
- ISM3 [18]: This management model of security and its maturity is oriented to implement an ISMS and define different security levels where each one of them can be the final objective of an organization.

When studying the existing literature we have found several attempts (see Figure 1) to solve the problem of applying the traditional ISMS systems to SMEs

centered in some aspects of ISMSs. In the following subsections, we will show some of the security management maturity models oriented to SMEs that are being developed. Although these models do not solve the existing problems, we consider that they make interesting contributions that must be analyzed. Among them, we can highlight the ones listed below: Eloff's proposal [19], Areiza's proposal [20], Dojkovski's proposal [21] and Sneza's proposal[22], IS2ME [23], Wiander and Holapa's proposal [24], Carey-Smith's proposal [25] and Tawileh's proposal [26].

In numerous bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs is detected and highlighted[27-30]. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified on repeated occasions. Moreover, organizations, even the big ones, tend more to adopt groups of processes related as a set than to deal with processes independently [31].

Therefore and to conclude 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 together with a tool that supports this model, taking as a basis the problem that this kind of companies face and that has lead to continuous failures in the implementation attempts into this kind of enterprises.

3 Characteristics of an ISMS Oriented to SMEs

The methodology for the management of security and its maturity in SMEs that has been 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.

In this section, we analyze the characteristics that an ISMS should have for its implementation and correct functioning within the SMEs environment. These characteristics have been obtained through a detailed analysis of the ISO27001 standard and the action research method. Eleven main characteristics that we have determined that an ISMS implementation methodology oriented to SMEs should have: Life cycle of the ISMS, Framework, Oriented culture of security, good practice guides, risk analysis and management, metrics, maturity level, oriented SMEs, reuse of knowledge, software tools available, and case studies. These eleven characteristics have been obtained through the application of the "*action research method*" to actual cases.

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 and reusability 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.

Table 1. Comparison of security management methodologies and desirable characteristics for ISMSs in SMEs.

	ISMS Cycle	Framework	Maturity level	Security culture	Guide of good practices	Risk analysis and management	Metrics	Oriented to SMEs	Reusing knowledge	Availability of a software tool	Practical cases
ISO/IEC27000	Yes	Yes	Yes	Parc	Yes	Yes	Parc	No	No	Parc	Yes
ISO/IEC15408/CC	No	No	Yes	No	No	No	Parc	No	No	Parc	Yes
ISO/IEC21827/SSE–CMM	Yes	Yes	Yes	No	No	Parc	No	No	No	Parc	Yes
ISO/IEC20000	Yes	Yes	No	No	Yes	No	No	No	No	Parc	Yes
ITIL	Yes	Yes	No	No	No	No	No	No	No	Parc	Yes
COBIT	Yes	Yes	No	Parc	Yes	Yes	Yes	No	No	Yes	Yes
ISM3	Yes	Yes	Yes	No	Yes	Parc	Yes	Parc	No	Parc	Yes
Eloff´s proposal	No	No	Yes	No	Yes	No	Yes	Yes	No	No	No
Areiza´s proposal	No	No	Yes	No	Yes	No	No	Yes	No	No	No
Dojkovski´s proposal	No	Yes	No	Yes	No	No	No	Parc	No	No	Parc
IS2ME	Yes	No	No	No	Yes	No	No	Yes	No	Parc	Yes
ASD	Parc	Parc	Yes	No	Yes	Parc	No	Yes	No	No	Parc
Carey-Smith proposal	Parc	No	No	No	Yes	No	No	Yes	Parc	No	No
Tawileh´s proposal	Yes	No	No	No	No	No	No	Yes	No	No	Yes
Sneza´s proposal	No	Yes	No	Yes	No	No	No	Parc	No	No	Yes
MMSM-SME	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

In Table 1, we can see a comparison of the different models, methodologies and guides to manage security analyzed in the previous section including the methodology we have developed with the desirable characteristics for SMEs. We consider that the considered aspects can be fully fulfilled, partially fulfilled or not taken into account by the model. Now, we will describe each one of the analyzed aspects:

- ***ISMS Cycle:*** The model describes clearly the development, implementation and maintenance phases of the ISMS. Commonly, models use the PDCA cycle.
- ***Framework:*** The model describes clearly all of the elements composing the ISMS once implemented.
- ***Maturity Levels:*** The model is oriented to the implementation of a progressive security based on levels.
- ***Security Culture:*** The model has taken into account the orientation to

securety culture and not only the technical and management orientation like the classical models.

- ***Guide of Good Practices:*** The model includes or considers the integration of a guide of good practices or security controls within the ISMS.
- ***Risk Analysis and Management:*** The model includes mechanisms for estimation and management of the risks to which the information system assets are exposed.
- ***Metrics:*** The model includes mechanisms for measuring the fulfillment of the security controls.
- ***Oriented to SMEs:*** The model has been developed thinking of the special case of SMEs.
- ***Reusing Knowledge:*** The model obtains knowledge from implementations in a way that this knowledge can be reused to facilitate further implementations.
- ***Availability of a Software Tool:*** The model is supported by a tool.
- ***Practical Cases:*** The model has been developed and refined from practical cases.

4 MMSM-SME Methodology

In this section, we offer a global vision of the set of subprocesses and activities composing the MMSM-SME methodology [32] and the standards and proposals used for creating it.

The MMSM-SME methodology includes all aspects considered desirable for SMEs including the automatization of security management models to reduce the system generation costs and a development completely oriented to SMEs; avoiding the generalization of other models.

Other advantage of MMSM-SME as compared to the rest of analyzed models is that it uses the knowledge obtained during different implementations to reduce the ISMS generation costs in similar companies. To do so, it uses the concept of "schemas". This is especially relevant because it allows the understanding of the relationships between the elements forming the enterprise information with the objective of managing its security[33].

This methodology is formed by three subprocesses:

- Subprocess P1 (GEGS – Generation of schemas). The main purpose of this subprocess is to allow the generation of a schema (structure formed by the main elements taking part in an ISMS and their relationships for a specific type of companies that share common characteristics -same sector and size- that can be used later to reduce time and cost of ISMS generation for a company.
- Subprocess P2 (GSGS – ISMS Generation): The main objective of this subprocess is to allow the generation of the elements that will form the security management system (ISMS) for a company, from a schema (structured generated through the GEGS subprocess) valid for a set of companies; performing this process at a reduced cost.

- Subprocess P3 (MSGS – ISMS Maintenance): The main objective of this subprocess is to allow and support the company to manage the information system security.

5 Conclusions and Future Works

In this paper, we have carried out a review of the different guides and methodologies for the management of security and its maturity in information systems as well as of the processes associated with the implementation of the classical security management systems.

Regarding the most outstanding standards, we have been able to prove that the majority of security management models have been based on the ISO/IEC17799 international standard and that the most successful security management models in big enterprises are ISO/IEC27001, COBIT and ISM3 but they are very difficult to implement and demand a too high investment that the majority of SMEs cannot make [13]. Although, new very interesting proposals oriented to this kind of companies are arising; they face problems in a very incomplete way.

In numerous bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs is detected and highlighted[29, 30]. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified on repeated occasions. Moreover, organizations, even the big ones, tend more to adopt groups of processes related as a set than to deal with processes independently [31].

The main problem of all management models of security and its maturity presented is that they are not being successful when being implemented into SMEs. This is mainly due to the following reasons:

- Some models were developed thinking of big organizations (ISO/IEC27001, ISO/IEC21827, Common Criteria, ISO/IEC20000, ITIL, COBIT) and of the organizational structures associated with them.
- Others (ISM3, Areiza's proposal, Eloff's proposal, ASD, IS2ME, Carey-Smith's proposal, Tawileh's proposal) have attempted to focus SMEs problems but they are incomplete models that only face part of the problem. Furthermore, most of them are theoretical models and are still being developed.

All these standards and proposals for security management are very important and their contributions have been taken into account for the development of the stated methodology.

As a result of this research, we have been able to obtain the set of characteristics that an ISMS oriented to SMEs should have and how we can face each one of these characteristics using different components of the most relevant standards and researches existing today.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557), financed by the Centre for Industrial Technological Development (CDTI), ORIGIN (IDI-2010043(1-5)) financed by the CDTI and the FEDER, BUSINESS (PET2008-0136) awarded by the Spanish Ministry for Science and Technology and MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) and SERENIDAD (PII11-0327-7035) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

1. Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research.* 2008.
2. Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. 43(7): p. 125-128.
3. Park, C.-S., S.-S. Jang, and Y.-T. Park, *A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance.* IJCSNS International Journal of Computer Science and Network Security., 2010. 10(3): p. 10-21.
4. Barlette, Y. and V. Vladislav. *Exploring the Suitability of IS Security Management Standards for SMEs*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008. Waikoloa, HI, USA.
5. Fal, A.M., *Standardization in information security management* Cybernetics and Systems Analysis 2010. 46(3): p. 181-184.
6. Wiander, T. and J. Holappa, *Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor. 2006.
7. Coles-Kemp, E. and R.E. Overill. *The Design of Information Security Management Systems for Small-to-Medium Size Enterprises.* in *ECIW - The 6th European Conference on Information Warfare and Security.* 2007. Shrivenham, UK: Defence College of Management and Technology.
8. Sánchez, L. E., et al. *MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs.* in *9th International Conference on Enterprise Information Systems (WOSIS'07).* 2007b. Funchal, Madeira (Portugal). June.
9. Sánchez, L. E., et al. *Developing a model and a tool to manage the information security in Small and Medium Enterprises*. in *International Conference on Security and Cryptography (SECRYPT'07)*. 2007a. Barcelona. Spain.: Junio.
10. Sánchez, L. E., et al. *Developing a maturity model for information system security management within small and medium size enterprises.* in *8th International Conference on Enterprise Information Systems (WOSIS'06)*. 2006. Paphos (Chipre). March.
11. Sánchez, L. E., et al. *SCMM-TOOL: Tool for computer automation of the Information Security Management Systems*. in *2nd International conference on Software and Data Technologies (ICSOFT'07)*. . 2007c. Barcelona-España Septiembre.
12. Sánchez, L. E., et al. *Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas.* in *International Conference on Security and Cryptography (SECRYPT'08)*. 2008. Porto–Portugal.
13. Velásquez, N. and M. Estayno. *Desarrollo y Mantenimiento Seguro de Software para Pyme: MoProSoft alienado a ISO/IEC 17799:2005*. in *IV Congreso Iberoamericano de Seguridad Informática (CIBSI'07)*. 2007. Mar de Plata. Argentina.: Noviembre.

14. ISO/IEC27001, *ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements.* 2005.
15. ISO/IEC20000, *ISO/IEC20000, Service Management IT.* 2005.
16. ITILv3.0, *ITIL, Information Technology Infrastructure Library.*, C.C.a.T.A. (CCTA). Editor. 2007.
17. COBITv4.0, *Cobit Guidelines, Information Security Audit and Control Association*. 2006.
18. ISM3, *Information security management matury model (ISM3 v.2.0)*. 2007, ISM3 Consortium.
19. 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: p. 130-136.
20. Areiza, K.A., et al., *Hacia un modelo de madurez para la seguridad de la información.* 3er Congreso Iberoamericano de seguridad Informática, 2005a. Nov, (2005): p. 429 - 442.
21. Dojkovski, S., S. Lichtenstein, and M.J. Warren. *Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises*. in *5th European Conference on Information Warfare and Security*. 2006. Helsinki, Finland: 1-2 June.
22. Sneza, D., L. Sharman, and W. Matthew John. *Fostering information security culture in small and medium size enterprises: An interpretive study in australia*. in *the Fifteenth European Conference on Information Systems*. 2007. University of St. Gallen, St. Gallen.
23. Linares, S. and I. Paredes (2007) *IS2ME: Information Security to the Medium Enterprise.* Volume,
24. Wiander, T. and J. Holappa, *Managing Information Security in Small and Medium-sized Organization,* in *Handbook of Research on Information Security and Assurancence*. 2007.
25. Carey-Smith, M.T., K.J. Nelson, and L.J. May. *Improving Information Security Management in Nonprofit Organisations with Action Research*. in *Proceedings of The 5th Australian Information Security Management Conference*. 2007. Perth, Western Australia: School of Computer and Information Science. Edith Cowan University.
26. Tawileh, A., J. Hilton, and S. McIntosh, *Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach*, in *ISSE/SECURE 2007 Securing Electronic Business Processes*, Vieweg, Editor. 2007. p. 331-339.
27. Batista, J. and A. Figueiredo, *SPI in very small team: a case with CMM.* Software Process Improvement and Practice, 2000. 5(4): p. 243-250.
28. Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. 6: p. 67-83.
29. Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. 9: p. 23-31.
30. Calvo-Manzano, J.A., *Método de Mejora del Proceso de desarrollo de sistemas de información en la pequeña y mediana empresa (Tesis Doctoral). Universidad de Vigo*. 2000.
31. Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. 7(3): p. 4-13.
32. Sánchez, L.E., et al., *MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES.*, in *V Congreso Iberoamericano de Seguridad Informática*. 2009: Montevideo, Uruguay.
33. Awad, E. and H. Ghaziri, *Knowledge Management*, ed. P. Hall. 2003.