Scmm-Tool - Tool for Computer Automation of the Information Security Management Systems.

Conference Paper · July 2007

Source: DBLP

CITATIONS
12

READS
171

4 authors, including:

Luis Enrique Sánchez Crespo
University of Castilla-La Mancha
89 PUBLICATIONS **262** CITATIONS
SEE PROFILE

Eduardo Fernández-Medina
University of Castilla-La Mancha
282 PUBLICATIONS **2,977** CITATIONS
SEE PROFILE

Mario Piattini
University of Castilla-La Mancha
1,101 PUBLICATIONS **11,365** CITATIONS
SEE PROFILE

SCMM-TOOL: Tool for computer automation of the Information Security Management Systems.

Luís Enrique Sánchez, Daniel Villafranca
SICAMAN NT. Departamento de I+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
{lesanchez, dvillafranca} @sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department. UCLM-Soluziona Research and Development Institute. University of Castilla-La Mancha, Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract: For enterprises to be able to use information technologies and communications with guarantees, it is necessary to have an adequate security management system and tools which allow them to manage it. In addition, security management system must have highly reduced costs for its implementation and maintenance in small and medium-sized enterprises (from here on refered to as SMEs) to be feasible. In this paper, we will show the tool we have developed using our model for the development, implementation and maintenance of a security management system, adapted to the needs and resources of a SME. Furthermore, we will state how this tool lets enterprises with limited resources manage their security system very efficiently. This approach is being directly applied to real cases, thus obtaining a constant improvement in its application.

1 INTRODUCTION

Information and processes supporting systems and nets are the most important assets for any organization (Dhillon and Backhouse 2000) and they suppose the main differentiating factor in the evolution of an enterprise. Nowadays, it is very complex for a small or medium-size enterprise to tackle the implementation of a security management system (Pertier 2003; Kim and I.Choi 2005). The tendency in the field of enterprise security is that of gradually migrating their culture towards the creation of a security management system (ISMS), despite the fact that this progression is very slow. Thus, studies such as that of René Sant-Germain (Sant-Germain 2005) estimate that with the current models, by 2009 only 35% of the enterprises in the world which employ more than 2000 people will have implemented an ISMS, and that the figures for SMEs will be much worse.

At present, the market demands that enterprises are able to guarantee that technologies for computer assets and information are secure, fast and easy to interact with (Corti et al. 2005). However, in order to fulfill these requirements, the system administrators have discovered two problems with no satisfactory solution: on the one hand, the lack of adequate tools that allow us to face information systems security in a centralized, simple and dimensioned according to the size of enterprises way and on the other hand, the lack of information security guides that let us answer the following questions: Where do I have to search?, What do I have to control? How do I have to control it? Today, this process finishes almost always giving place to the fact that enterprises take the risk of lacking of a security management system due to their inability to implement it.

Organizations, both national and international, have made an effort to elaborate a set of regulations and specifications related to security in information and communication technologies to solve the second problem and in spite of the fact that today we can find in the market hundreds of tools oriented to security, none of them is on its own a complete and efficient solution for this kind of systems in the case of SMEs.

In this paper, we shall describe a new tool that we have developed from our maturity and security management model oriented to SMEs that tries to

solve the problems detected in classical models and tools 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 analysed in detail in the following sections of the paper.

The remainder of this paper is organized as follows: Section 2, very briefly describes existing tools for security management their current tendencies and some of the new proposals that are appearing. Section 3, introduces our proposal for a tool for security management orientated towards SMEs. Finally, in Section 4, we shall conclude by discussing our future work on this subject.

2 RELATED WORK

Nowadays, there is a wide set of tools associated with ISMS whose objective is to attain the security goals proposed in the different Maturity and Security Management models (COBIT 2000; Eloff and Eloff 2003; Lee et al. 2003; Aceituno 2005; Areiza et al. 2005; Barrientos and Areiza 2005). These tools and guides can be grouped into the following set of tools:

- ***Risk Analysis Tools:*** At present, the tools most used for risk analysis are PILAR and EAR, based on Magerit v2 (MageritV2 2005). Other tools used are, firstly, that proposed by ENISA, secondly, the OCTAVE-S and Octave Automated Tool which implements the OCTAVE (Alberts and Dorofee 2001) risk evaluation methodology and finally, CRAMM and COBRA.
- ***Orientated towards management:*** At present, this set of tools is formed of guides. Among these, we can highligh that of information security for NIST managers and other tools such as TDBSSI which belong to the French Government.
- ***Auto-evaluation Tools:*** This set of tools is basically composed of fulfillment check-lists, and among them we can highlight the auto-evaluation questionnaire for the verification of control state(ISO/IEC17799 2005) from the SANS Institute and the BITs tool for the evaluation of the operational risk of information security.
- ***For ISMS implementation:*** Among the tools of which this set is composed, we can highligh AWICMSM, Callio Secura 17799 based on (ISO/IEC17799 2005), (BS7799 2002) and (UNE71502 2004) and Proteus, a piece of software covering all the phases of an ISMS implementation.
- ***For Policies implementation:*** We can highlight Toolkit of the Universities and Colleges Information Systems Association based on (BS7799 2002) and the guides dealing with the technical aspects of NIST information security.
- ***For conciousness and sensibilization:*** Nowadays, this set of tools is formed of guides such as those of ENISA or NIST (Wilson and Hash 2003) which are used for the creation of an information security consciousness plan.
- ***Orientated towards business continuity:*** Despite the fact that that there are some applications such as Office Shadow, LDRPS, eBRP, IMCD, the majority of enterprises use guides such as those offered by NIST (Swanson et al. 2002) or the British Standard (BS25999 2006).

Each of these tools is focused upon a single aspect of ISMS instead of upon the whole set. Siegel (Siegel et al. 2002) points out that computer security models which are exclusively centered upon risk elimination models are not enough. On the other hand, Garigue (Garigue and Stefaniu 2003) highlights the fact that at present, managers not only wish to know what has been done to mitigate risks, but that it is also necessary to explain to them in as efficient a way as possible that this task has been carried out and whether or not it has been possible to save money.

The problem of these tools is that they are a set of partial and complex solutions to the stated problems, and it is for this reason that they are unsuccessful when implemented in SMEs, principally because they were developed with large organizations in mind, where associated costs are not critical. This makes them inadequate for an SME environment.

The proposal presented in this paper is also based on the ISO/IEC 17799 international regulation but has been orientated towards its application in SMEs and an avoidance of the problems detected in current tools.

3 SCMM-TOOL: TOOLS FOR ISMS IN SME

The application that must support the Information Security Maturity Model that we propose allows any organization to evaluate the state of its security but

is mainly orientated towards SMEs through developing the simple, cheap, fast, automated, progressive and sustainable security management models that are the main requirements of this kind of enterprises at the time of implementing these models.

From the user's viewpoint, our model presents two clear advantages:

- ***Simplicity:*** All of the ISMS phases are orientated towards reducing the complexity of the ISMS management process, by bearing in mind organizations whose organizative structures are very simple.
- ***Automation:*** The whole system uses schemas which enable the automation of the necessary processes for ISMS.

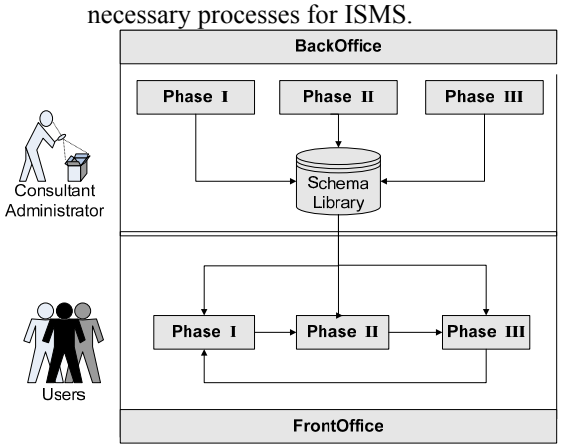

Figure 1: Application Architecture

The model is composed of two clearly differentiated parts (see Figure 1):

- ***BackOffice:*** Whose central nucleus is the ***Schema Generator for ISMS's***. By using this tool, we can generate complete schemas which allow us to automate the most complex and expensive parts of ISMS.
- ***FrontOffice:*** This allows users to generate ISMS's at the highest level of automation and simplicity from a previously generated schema.

In Figure 1, we can see how at the BackOffice administrated by the consultant, three-phases schemas are defined and stored in the schema library. At the same time, users define at the FrontOffice the ISMS for their enterprise through a feedbacked three-phases cycle that takes as a basis for its generation a schema from the schema library.

In the BackOffice administrated by the consultant, three-phase schemas are defined and stored in the schema library. At the same time, users in the FrontOffice define the ISMS for their enterprise through a feedbacked three-phase cycle which takes a schema from the schema library as a basis for its generation.

In each of the phases of the BackOffice, the schema that will later be used in the same phase of the FrontOffice to generate the data for an ISMS instance is defined. The **schemas** are the core upon which our model is developed, owing to the fact that they allow the automation of the ISMSs. These **schemas** consist of a set of objects and matrices which are defined from experience and practice derived from working with customers.

On the other hand, against the classical model of tools that are installed on the customer's enterprise, SCMM-TOOL has been developed through web technology in a way that it can offer SMEs access through the internet following the ASP business model (see Figure 2). This model has been chosen since it presents several advantages as compared to the traditional models:

- Elimination of the cost of installing the application on the customer's enterprise.
- Access to new versions without additional costs.
- It eliminates the need of infrastructure.
- It facilitates the existence of external auditors.

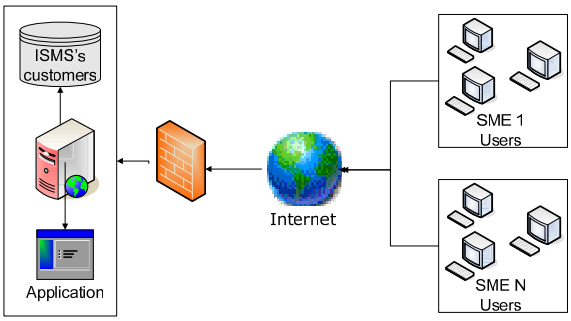

Figure 2: Business model Architecture

Thus, with a low cost of initial configuration and a small monthly fee, SMEs have access to a complete system of management of their security system.

Nowadays, we are studying the possibility of including in the model some variations that allow customers to maintain their data locally to increase their confidence and security level.

3.1. Schema Generator.

The schema generator is one of our model's main contributions, and could be considered as the main nucleus of the application. The tool allows us define schemas with which to perform the research process within the enterprises. This then allows us to carry out small adjustments to these schemas until we

obtain the schema that is best adapted to each type of enterprise.

At present, the tool is composed of only one schema which has been obtained through a successive refinement achieved through the application of the model to diverse SICAMAN customers and a subsequent analysis of the results obtained.

The schemas are defined through three phases:

- ***Phase I:*** Maturity factors, the weight-factor matrix and a set of controls are defined.
- ***Phase II:*** The type of assets, threats, vulnerabilities, impact criteria and risk matrixes are defined.
- ***Phase III:*** Object library, matrixes of associations between objects and controls, regulations, procedures and their phases, and metrics are defined.

Additionally, the system will be formed by other objects necessary for their functioning:

- ***Profiles:*** Profiles define the set of necessary roles for the system to work. Given that the application is oriented to SMEs, we have selected a small set of roles: Administrator, User, Security Manager, System Manager, System Department, Development Manager, Explotation Manager, HR Manager, Marketing Manager Assets Owner and General Manager.

Only users belonging to one of these roles will be affected by the security system. An user can have several roles assigned. Roles are very important since the automatic flow of procedures is supported by them.

3.1.1. Phase I: Creation of the schema for maturity level establishment.

This phase will allow us to define the set of levels, factors and controls necessary for establishing the current and the desirable maturity level (see Figure. 3).

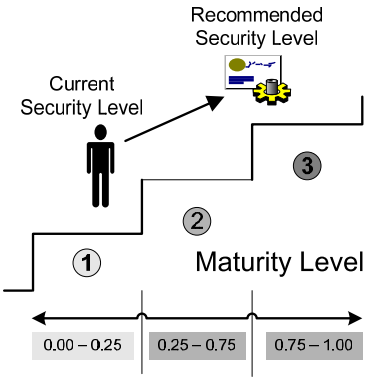

Figure 3: Current and target maturity level.

The main objects of which this phase of the system is composed are as follows:

- ***SectorFactor Matrix:*** The current matrix contains 354 weights which allow us to carry out a correction factor for each of the sectors and to a factor of the set of defined factors influencing the enterprise's security.
- ***Maturity Rules:*** The current schema is formed of 6 factors, each having 3-4 selection criteria. Both the maturity rules the Sector-Factor matrix will allow us to determine the desirable level of maturity.
- ***Maturity Levels:*** The system permits the definition of different maturity levels. Nowadays, an entire schema based on a three maturity level model has been developed.
- ***Set of controls:*** This set of controls is based on the 127 controls of ISO17799:2000 but has been increased to achieve a set of 735 subcontrols which allow us to obtain the level of security for each control with a higher level of accuracy.

3.1.2. Phase II: Creation of the schema for risk analysis.

This phase will allow us to define the set of necessary objects which will enable us to carry out a basic risk analysis of the enterprise's assets in a minimum period of time. The model obtained uses the list of assets to allow the system to be able to perform a risk analysis and control.

The objects of which this phase is formed are described below:

- ***Type of Assets:*** We have defined 23 types of assets for the current schema.
- ***Threats:*** For the current schema, a set of 51 threats associated with 6 types of threats have been defined.
- ***Vulnerabilities:*** For the current schema, 48 vulnerabilities have been defined.
- ***Risk Criteria:*** For the current schema, we have defined 4 criteria (Confidentiality, Integrity, Availability and Legality).
- ***Type of assets vs vulnerabilities matrix:*** This allows us to associate assets with the vulnerabilities that may affect them. In the current schema, we have defined 252 relationships for this matrix.
- ***Threats vs vulnerabilities Matrix:*** This allows us to associate vulnerabilities with each type of threat. With this matrix, we can also associate threats and assets through the assets-vulnerabilities matrix. In

the current schema, 79 relationships have been defined for this matrix.

- ***Threats vs ISO17799 controls Matrix:*** We can associate threats with the ISO17799 controls that affect them. Thanks to the previous matrixes, we can also give a security level to an asset by using the controls associated with it. In the current schema, 940 relationships have been defined for this matrix.
- ***Type of Assets-Vulnerabilities vs Risk Criteria Matrix:*** This matrix allows us to associate the type of assets and vulnerabilities of an enterprise with respect to the risk criteria that we have defined. In the current schema, 345 relationships have been defined for this matrix

3.1.3. Phase III: Creation of the ISMS object schema.

This phase defines the library of objects of which the ISMS is composed. It also defines their properties. Each of the defined objects has a set of additional associated properties (periodicity, etc) which will be useful for dynamically recalculating the level of fulfillment of controls.

The objects defined in this phase have an associated set of properties (a schema, a section and a version). The current schema is formed of an object library composed of the following set: 50 procedures, 4 technical instructions, 25 regulations files, 67 patterns and 36 registers.

Each of the defined objects has had two temporality values assigned to it:

- ***Estimated periodicity:*** This represents an estimation of the time in which an object must be used at least once. When the estimated periodicity is exceeded, the system will punish the current level of fulfillment of the controls associated with that object, decreasing them according to an estimated percentage.
- ***Compulsory Periodicity:*** The object can have this temporality value defined or not. This represents the period of time in which the object must be compulsory executed at least once. When the compulsory periodicity is exceeded, the system will punish the current level of fulfillment of controls associated with that object decreasing them according to an estimated percentage.

The periodicities defined in the objects, together with the complaint process, the periodical audits and the metrics are in charge of dynamically revaluating the state and evolution of the system.

In the current version of this application, we have taken into consideration two special types of objects (regulations and procedures):

- ***Regulations:*** There is a set of regulations with which the enterprise must comply. Each regulation is associated with the controls through a matrix. This allows the updatedness of the value of fulfillment of them when an unfulfillment of a regulation is detected. In the current schema there are 264.
- ***Procedures:*** Procedures may be carried out by a set of users from the enterprise according to the profiles that they have been assigned. Each of these procedures has been assigned a set of phases through which users must pass in order to be able to fulfill the procedure. The current schema is composed of 50 procedures with a total of 609 phases with 697 possible execution paths. Each one of the phases of the procedure has a set of profiles associated with users that are in charge of approving the phases to allow that the procedure initiates a new phase assigned to it.

3.2. ISMS Generation

When a consultant aims to generate an ISMS for an enterprise by using the application and methodology that we have developed, he/she could do so in a minimum period of time and with minimum cost. To do this, he/she must pass through three phases in which a minimum of necessary information from both the selected schema and the algorithms defined in the application must be introduced, in order for the system to generate an ISMS which is adequate for the enterprise.

3.2.1. Maturity Level Establishment

This is the initial phase and it will require more information than the rest of phases due to the fact that it is necessary to define the enterprise profile (the enterprise's data and the valoration of the defined parameters) and the enterprise's current security level (through a checklist composed of 735 questions based on ISO/IEC 17799:2000).

As a result of this phase, a percentage of fulfillment of each control for each maturity level of the selected model will be achieved, together with the level which it is desirable to reach. If we have security controls over the current security level and the desirable security level, they will be taken into account at the time of the ISMS generation at phase

III, but it must be made clear to the users that these are optional since they are an overdimensioning of the enterprise's current security.

3.2.2. Risk level establishment.

In this phase, and thanks to the previous creation of the schema, we will only have to define the enterprise's set of assets (see Figure 4).

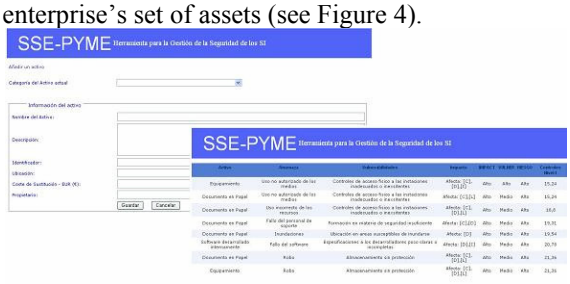

Figure 4: Risk module screens.

Once this set of assets has been defined, the system will apply two algorithms to generate the results of this phase:

- ***Risk matrix generation Algorithm:*** The risk matrix is automatically generated from the list of assets generated through the vinculation between the matrices of the selected schema and the algorithm application.
- ***Improvement Plan Generation Algorithm:*** The improvement plan will be generated using the report from phase I, together with an improvement report based on the result of the risk matrix. This report will be formed by the following parts: i) phase I report, ii) report of risk by assets, iii) risk improvement plan.

3.2.3. ISMS Generation.

In this phase, the system does not require additional information, as the ISMS most adequate for the enterprise is generated totally automatically through the **ISMS's generation algorithm**. This algorithm takes as:

- ***Compulsory:*** Those objects directly affected by the controls of the nearest target security level.
- ***Optional:*** Those objects belonging to levels that must be reached in a short period of time or to already reached levels which are different from the current target level (overdimensioning).
- ***Disposable:*** Those objects which do not make sense for this type of enterprise and whose implementation may cause the destabilization of the ISMS by incurring excessive costs.

The resulting product of this phase will be a set of asset procedures with a series of associated phases, objects and profiles.

3.2.4. Working with ISMS.

The enterprise's real work starts once we have generated the ISMS. So far, and thanks to the use of schemas, the consultant has been able to define a management system which is adequate for the enterprise and is also affordable. Now, the enterprise must begin to work with the system.

The work with the proposed security management system has been developed considering simplicity. For that reason, users must know a maximum of 50 procedures and around 250 regulations. Not all users must know those 50 procedures since the majority of them can only be used by the person in charge of security or members of the system department. In general, users must only know the existence of a small set of procedures.

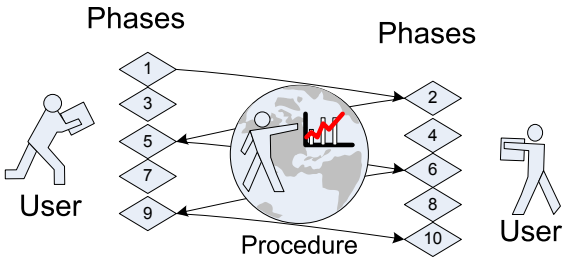

Figure 5: Procedure Flow

When a user requires the use of an asset or the performance of an operation that may affect the security of the enterprise's information system, he/she will start the SCMM-TOOL and will obtain a list of the procedures that he/she can activate. Once the desired procedure has been selected (see Figure. 5), the system will automatically activate the phases and will ask each of the users involved for the necessary operations to move from one phase to the following one. In this way, the person in charge of a phase must approve it; otherwise, the procedure will be pending and the system will store the caused delays for a subsequent analysis.

When a user starts the system, he/she is always able to see the state of the procedures in which he/she is involved and those that are delayed because of him/her.

There is a special procedure called "***Complaint Procedure***" This procedure (see Figure. 6) manages the complaints made by the system user about the

non-fulfilment of a regulation. The person in charge of security will determine whether the complaint is justified or not. If it is considered to be justified, the system will automatically decrease the level of security of the controls associated with that regulation.

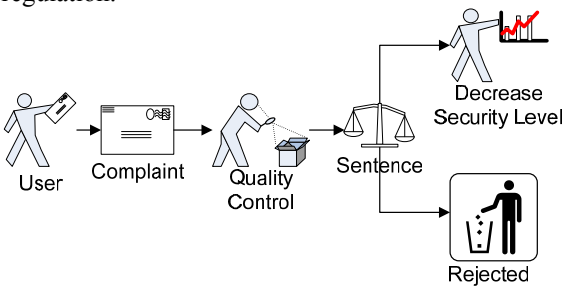

Figure 6: Complaint Procedure Schema

3.2.5. ISMS evolution.

Our ISMS model has been designed to evolve dynamically without being compulsory although the participation of external auditors is advisable. Thus, our model does not have to wait for external auditors to arrive in order to know how the system evolves but the system constantly evolves by changing the level of security of the controls and readjusting all the phases of the system.

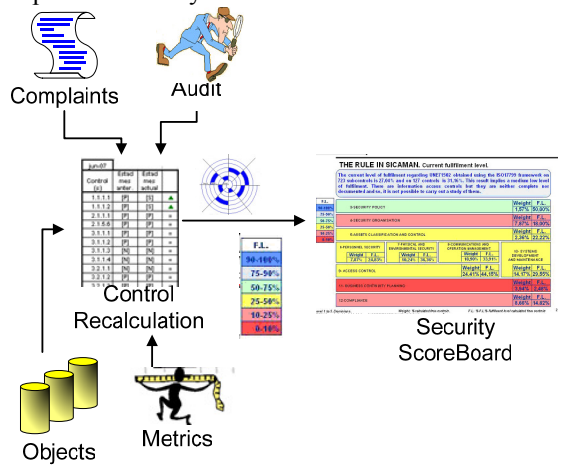

Figure 7: ISMS updatedness Factors

The current version of the application evolves by taking four aspects into account (see Figure. 7): i) object periodicity, ii) complaints, iii) set of metrics and iv) external audits. With regard to these factors, the system recalculates the controls and adapts the enterprise's security control panel.

4 CONCLUSIONS AND FUTURE WORK

Despite the enormous efforts that are being made to create adequate maturity models to manage security in SMEs, these do not yet fit properly with the environment in which they must be implemented. The most possible reason is the lack of maturity of enterprises as well as the lack of specialized tools in this kind of enterprises. Even when there are tools in the market, they do not offer a total solution and have to be completed with other tools and guides converting enterprises' information system security into a set of heterogeneous and non-integrable applications that force the enterprise to invest huge amounts of resources for its maintenance.

In this paper, we have presented a proposal for a new maturity and security management tool orientated towards SMEs which allows us to reconfigure and adapt existing models in order to guarantee the security and the stability of their management system with regard to the dimension of each enterprise. To do so, we have defined a methodology and a tool able to support the results that have been generated during the research. It has been clearly defined how the application uses the developed model to reach the objects as well as the improvements that it offers as compared to the classical systems.

The presented application reduces the system's implementation costs and also improves the percentage of success of its implementation in SMEs. For these reasons, as the majority of our customers are SMEs, our proposal is being well received and its application is being very positive because it allows this type of enterprises access to the use of security maturity models which, until now, has only been possible for large enterprises. Moreover, with this model, we can obtain short-term results and reduce the costs that imply the use of other models, obtaining a higher degree of satisfaction of the enterprise.

Given that our proposal is being constantly developed, our medium and long term objective is too deep into the maturity models to refine our model, improving the level of automatization of the tool.

Among the model improvements that we intend to work on in the future, it is worth highlighting that we wish:

- To improve the algorithms of which the system is composed in order to increase their effectiveness in decision making.
- To include a planner of the time and the resources that the company wants to spend

on the project, so that the system will be able to estimate time-milestones in the improvement plan.
- In Phase III, to include a library with the subprojects that should be worked on to improve the security management system globally.

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

ACKNOWLEDGEMENTS

This research is part of the following projects: DIMENSIONS (PBC-05-012-1) and MISTICO (PBC-06-0082), both supported by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", RETISTRUST (TIN2006-26885-E) granted by the "Ministerio de Educación y Ciencia" (Spain), and Proyect SCMM-PYME (FIT-360000-2006-73) supported by the PROFIT granted by the "Ministerio de Industria, Turismo y Comercio).

REFERENCES

Aceituno, V. (2005). "Ism3 1.0: Information security management matury model."

Alberts, C. J. and A. J. Dorofee (2001). OCTAVE Criteria, Version 2.0.

Areiza, K. A., A. M. Barrientos, et al. (2005). Hacia un modelo de madurez para la seguridad de la información. IV Congreso Internacional de Auditoría y Seguridad de la Información.

Barrientos, A. M. and K. A. Areiza (2005). Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad. Master's thesis, Universidad EAFIT.

BS7799 (2002). BS 7799: Information security management systems. .

BS25999 (2006). BS25999 - Standard for Business Continuity Management.

COBIT (2000). Cobit Guidelines, Information Security Audit and Control Association.

Corti, M. E., G. Betarte, et al. (2005). Hacia una implementación Exitosa de un SGSI. IV Congreso Internacional de Auditoría y Seguridad de la Información.

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM **43**(7): 125-128.

Eloff, J. and M. Eloff (2003). 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.

Garigue, R. and M. Stefaniu (2003). "Information Security Governance Reporting." Information Systems Security **sept/oct**: 36-40.

ISO/IEC17799 (2005). ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management.

Kim, S. and I.Choi (2005). Cost-Benefit Análisis of Security Investments: Methodology and Case Study. ICCSA 2005, LNCS 3482.

Lee, J., J. Lee, et al. (2003). A CC-based Security Engineering Process Evaluation Model. Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC).

MageritV2 (2005). Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2.

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

Sant-Germain, R. (2005). "Information Security Management Best Practice Based on ISO/IEC 17799." Setting Standars, The information Management JournaL **39**(4): 60-62, 64-66.

Siegel, C. A., T. R. Sagalow, et al. (2002). "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security." Security Management Practices **sept/oct**: 33-49.

Swanson, M., A. Wohl, et al. (2002). "Contingency Planning Guide for Information Technology Systems." NIST.

UNE71502, A. (2004). UNE 71502:2004 - Tecnología de la Información. Especificaciones para los sistemas de gestión de seguridad de la información.

Wilson, M. and J. Hash (2003). "Building and Information Technology Security Awareness and Training Program." NIST **Special Publication 800-50**.