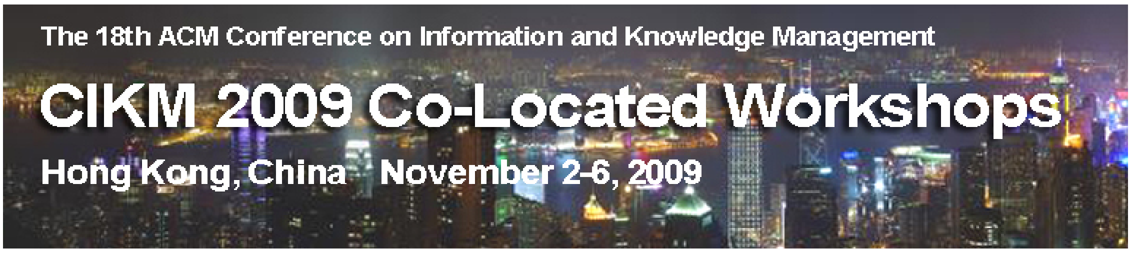
CD Main Page
CloudDB'09
CNIKM'09
DOLAP'09
DSMM'09
DTMBio'09
MoSE+DQS'09
PaIR'09
PAVLAD'09
SWSM'09
TSA'09
WIDM'09


The 18th ACM Conference on Information and Knowledge Management
CIKM 2009 Co-Located Workshops
Hong Kong, China November 2-6, 2009

MoSE+DQS'09 Table of Contents

(Return to Top)

MoSE+DQS 2009 Workshop Organization

Program Chairs:
Esperanza Marcos *(Rey Juan Carlos University, Spain)*
Mike Papazoglou *(Tilburg University, The Netherlands)*
Mario Piattini *(University of Castilla – La Mancha, Spain)*

Steering Committee Chairs:
Ma. Valeria de Castro *(Rey Juan Carlos University, Spain)*
Belén Vela *((Rey Juan Carlos University, Spain)*
Ismael Caballero *(University of Castilla – La Mancha, Spain)*
Manuel Serrano *(University of Castilla – La Mancha, Spain)*

Steering Committee:
Acuña, César *(Rey Juan Carlos University, Spain)*
Bollati, Verónica *(Rey Juan Carlos University, Spain)*
Cuesta, Carlos *(Rey Juan Carlos University, Spain)*
Herrmann, Elisa *(Rey Juan Carlos University, Spain)*
López, Marcos *(Rey Juan Carlos University, Spain)*
Vara, Juan Manuel *(Rey Juan Carlos University, Spain)*

Program Committee:
An, Yuan *(Drexel University, USA)*
Atzeni, Paolo *(Università Roma Tre, Italy)*
Benatallah, Boualem *(University of New South Wales, Australia)*
Bézivin, Jean *(Université de Nantes, France)*
Bræk, Rolv *(University of Science and Technology, Norway)*
Calero, Coral *(University of Castilla – La Mancha, Spain)*
Cappiello, Cinzia (*Politecnico di Milano, Italia)*
Cardoso, Jorge *(SAP Research CEC Dresden, Germany)*
Caro, Angélica *(University of Bio-Bio, Chile)*
Casati, Fabio *(University of Trento, Italy)*
Castro, Alfonso (*Telefonica I+D, Spain)*
Corchuelo, Rafael *(University of Seville, Spain)*
Curbera, Francisco *(IBM T.J. Watson Research Center, USA)*
Embury, Suzanne *(University of Manchester, UK)*
Farinha, Jose (*ISCTE, Portugal)*
Fernandez, Eduardo *(Florida Atlantic University, USA)*
Fernández-Medina, Eduardo *(University of Castilla – La Mancha, Spain)*
Hamou-Lhadj, Abdelwahab *(Concordia University, Canada)*
Herrera-Viedma, Enrique *(University of Granada, Spain)*
Johannesson, Paul *(Stockholm University and Royal Institute of Technology, Sweden)*
Koch, Nora *(Ludwig-Maximilians-University Munich, Germany)*
Koronios, Andy *(University of South Australia, Australia)*
Lycett, Mark *(Brunel University, United Kingdom)*
Moraga, Marian *(University of Castilla – La Mancha, Spain)*
Pavon, Juan *(Complutense University of Madrid, Spain)*

Program Committee (continued):

Rodríguez, Alfonso *(University of Bio-Bio, Chile)*
Sauveron, Damien *(University of Limoges, France)*
Su, Yin *(Tsinghua University, China)*
Vallecillo, Antonio *(University of Malaga, Spain)*
Van den Heuvel, Willem-Jan *(Tilburg University, Netherlands)*
Vargas Solar, Genoveva *(CNRS, LSR-IMAG, France)*
Yonke, CL *(Aera Energy, USA)*

Additional reviewer: Pirzadeh, Heidar

Sponsors: sigweb

SIGIR
Special Interest Group
on Information Retrieval

Supporters: Universidad Rey Juan Carlos

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Foreword

These proceedings include the papers accepted for the *First International Workshop on Model Driven Service Engineering and Data Quality and Security (MoSE+DQS 2009)*, which was held in Hong Kong, on November 6th 2009.

This workshop included two different tracks focusing on Model Driven Service Engineering (MoSE track) and Data Quality and Security (DQS track).

Regarding the first issue we can see that Model-Driven Engineering (MDE) deals with the provision of models, transformations between them and code generators to address software development. One of the main advantages of model-driven approaches is the provision of a conceptual structure where the models used by business managers and analysts can be traced towards more detailed models used by software developers. This kind of alignment between high level business specifications and the lower level Service Oriented Architectures (SOA) is a crucial aspect in the field of Service-Oriented Development (SOD) where meaningful business services and business process specifications are those that can give support to real business environment usually changing with increasing speed. SOD has become currently in one of the major research topics in the field of software engineering, leading the appearance of a novel and emerging discipline called Service Engineering (SE), which aim to bring together benefits of SOA and Business Process Management (BPM). SE focuses on the identification of service (a client-provider interaction that creates value for the client) as first class elements for the software construction. The convergence of SE with MDE holds out the promise of rapid and accurate development of software that serves software users' goals.

On the other hand, Information technologies are becoming one of the most important aspects for organizations. The business value of the data stored in the company databases has been growing to become one of the most important assets of the company. These data represent one crucial asset for tactic, strategic and operational decisions. Due to this important role of the data, companies should assure the access to the data to several users guaranteeing the right levels of quality they need to accomplish the task they have to do.

Data Quality is a crucial issue in assessing the quality of business decisions support systems. Many aspects are related with the quality of the data, such as integrity, completeness, actuality and several other factors that make this kind of quality a multidimensional issue and a difficult issue. Data Security is another crucial aspect on information systems, not only because it affects Data Quality, but also because current information systems store sensitive and private data that should be treated rightly. Also, as Data Quality and Data Security are not independent concepts, the relationship between both concepts is worth being analyzed in order to give organizations some tools that can help in assuring both data dimensions.

The Workshop on Model Driven Service Engineering and Data Quality and Security intends to provide a forum for researchers and practitioners working on different issues related to SE in conjunction with MDE, boarding open research problems in this area as well as practical experiences. The workshop is also focused on auditing, measuring, predicting, evaluating, controlling, assuring and improving the quality and security of data. Particular interests include methods, modelling languages, development methodologies and techniques in these fields.

The six full papers (an acceptance rate of 54.5%) and four short papers were selected very carefully by the Program Committee in order to ensure a high quality workshop.

We wish to thank all the contributors to MoSE+DQS'09, in particular the authors who submitted papers and likewise, we acknowledge the time and effort contributed by all the members of the Program Committee who have very carefully reviewed the submitted papers.

We hope that you will find this program interesting and that the workshop will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

Esperanza Marcos
Mike Papazoglou
MoSE Program Committee Chairs

Mario Piattini
DQS Program Committee Chair

Ma. Valeria de Castro
Belén Vela
MoSE Organization Chairs

Ismael Caballero
Manuel Serrano
DQS Organization Chairs

Management of Scorecards and Metrics to Manage Security in SMEs

Luis Enrique Sánchez, Daniel Villafranca
Departament of R+D.
SICAMAN Nuevas Tecnologías.
13.700 Tomelloso
Lesanchez@sicaman-nt.com
Dvillafranca@sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
Alarcos Research Group
University of Castilla-La Mancha
13.071 Ciudad Real
Eduardo.FdezMedina@uclm.es
Mario.Piattini@uclm.es

ABSTRACT

Information Society depends more and more on Information Security Management Systems (ISMSs) and the availability of these systems has become vital for the evolution of Small and Medium Enterprises (SMEs). However, this kind of enterprises requires that ISMSs are adapted to their special characteristics and optimized from the viewpoint of the necessary resources to implement and maintain them. This paper presents the mechanisms included in the security management methodology for SMEs called MGSM-PYME that enables the responsible for security to have at all times knowledge of the level of security management of the enterprise. This model is being directly applied to real cases, thus obtaining a constant improvement in its application.

Categories and Subject Descriptors

D.2.8 [Metrics]: Process metrics.

General Terms

Measurement, Security.

Keywords

ISMS, Metrics, SME.

1. INTRODUCTION

The majority of enterprises have chaotic security systems that have been created without adequate guides or documentation and with insufficient resources. The classic controls seem to be insufficient on their own to provide us with minimum security guarantees. The security tools existing in the market help us solve part of the security problems but they never face the problem in a global and integrated way. Finally, the huge diversity of these tools and their lack of integration imply an enormous cost in resources to be able to manage them.

Experience has shown that for enterprises to be able to use information and communication Technologies with guarantees, it is necessary to have guides, metrics and tools that allow them to know at all times their security level and the vulnerabilities that have not been covered yet [1]. In SMEs, the application of security regulations has to face the additional problem of not having enough human and economic resources to perform an appropriate management.

According to recent researches [2], the success of ISMSs mainly depends on the following factors: i) approach security towards business; ii) implement security taking into account the enterprise culture; iii) achieve the indisputable, visible and compromised support of the enterprise management team ; iv) be able to understand properly security and evaluation requirements and risk management; v) make the management team as well as the rest of employees aware of the need of security; vi) offer all the organization training and guides about policies and regulations; vii) define a measurement system to evaluate the performance of the security management as well as suggest improvements. Regarding SMEs, these factors are important but also the ISMS must be optimized with reference to necessary resources and besides, its reach must be enough not to overlook security but not excessive to control its cost. For that reason, it is very important to have methodologies for information security management not only that are especially designed for this kind of enterprises but also that allow us to reuse knowledge in a way that their implementation is faster, more certain and cheaper.

In this paper, we will focus on the seventh of those factors, "define a measurement system to evaluate the performance of the security management as well as suggest improvements" adapting it for SMEs to achieve a very low maintenance cost offering the responsible for security the maximum possible value, allowing him/her to know how the fulfilment level of the different controls evolves at short term.

The paper continues with section 2, briefly describing how this problem is faced by each one of the main methodologies and models for security management existing today and their current tendency. In section 3, we will briefly introduce our proposal of methodology for security management oriented to SMEs called MGSM-PYME. In section 4, we will present the process used in MGSM-PYME to know and maintain the level of security in a

MoSE+DQS'09, November 6, 2009, Hong Kong, China.
Copyright 2009 ACM 978-1-60558-816-2/09/11...$10.00.

dynamic way. Finally, in section 5, we will conclude by indicating our future work.

2. RELATED WORK

With the purpose of reducing the lacks shown in the previous section and the losses caused by them, a huge number of processes, frameworks and information security methods have appeared and the need to implement them is being more and more known and considered by organizations but they are inefficient for SMEs as it has been shown.

In relation to the more highlighted standards, it has been proved that the majority of security management models are based on the international standards ISO/IEC17799 and ISO/IEC27002 and that the security management models that are being more successful in big enterprises are ISO/IEC27001, COBIT and ISM3, but they are very difficult to implement and require a too high investment that the majority of SMEs cannot make [3-5]. Although very interesting new proposals oriented to this kind of enterprises are arising, they face problems in a very incomplete way.

In numerous bibliographic sources, the difficulty that SMEs have if they try to use methodologies and maturity models for traditional security management that have been created for big enterprises [3-6] is detected and highlighted. Many times, authors justify the fact that the application of this kind of methodologies and maturity models is difficult and expensive for SMEs. Additionally, organizations, even the big ones, tend to adopt groups of processes related as a set to be treated independently [7].

Among the main standards that try to carry out a process of metrics within the ISMS, we can highlight those stated below:

- *ISO/IEC FCD 27004 [8]:* The 27000 series is a set of standards developed- or being developed- by ISO (International Organization for Standardization) and IEC (International Electrotechnical Comission)- that provide us with an information security management framework. Within this family, we can find ISO/IEC27004 that is at the developmental stage. It will specify the metrics and measurement techniques applicable for determining the efficiency of an ISMS and that of the related controls. These metrics are mainly used for the measurement of the components of the "Do" stage (implement and use) of the PDCA cycle.
- *ITIL [9]:* Information Technology Infrastructure Library (ITIL) is a wide set of management procedures created to help organization achieve quality and efficiency in IT operations. These procedures cover suppositions related to IT infrastructure, development and operations. ITIL attempts to cover, although in a very poor way, the services related to security management. Concerning metrics, organizations that work following ITIL good practices will see this aspect noticeably simplified because commonly they have adopted a culture of strategic support to the Management team through scorecards, through the definition and control of performance indicators (KPI) and those of fulfilment (KGI), among others.
- *COBIT [10]:* COBIT (Control Objectives for Information and Related Technology) is the methodology for IT governance developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). Objectives and metrics are defined in Cobit at three levels: i) IT metrics and objectives that define what the business expects from IT (measurement by business): ii) Metrics and Objectives of Processes that define the necessary delivery of the IT process to let us reach IT objectives (measurement of the process in IT); iii) Metrics of performance of the process (to indicate whether the objectives will be fulfilled or not). Cobit mainly uses two types of metrics: KPIs (number of incidences solved by Service Desk) and KGIS (average time of solving incidences).
- *ISM3 [11]:* This management model of security and its maturity is oriented to implement an ISMS as well as to define different security levels where each one of them can be the final objective of an organization. ISM3 contains a small set of metrics of management of processes oriented to the continuous improvement of the process since there are criteria to measure the effectiveness and efficiency of the information security management systems.

The problem of all the metrics defined by the main standards is that they are considered as something isolated from the rest of the system without integrating them into the global functioning of it with the aim of obtaining better information of the state of the security level of the controls at every moment. This makes them loose part of the importance that they could have for the responsible for security.

Therefore and as a conclusion of this section, we can state that it is appropriate and relevant to face the problem of developing a set of metrics that allow us to know at all times the level of fulfilment of security of the ISMS controls and update them dynamically, thus saving costs.

3. MGSM-PYME: Overview

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 these organizations have the greatest failure rate in the implementation of the existing security management methodologies.

One of the objectives pursued by the MGSM–PYME methodology is that of being easy to apply and that the model developed over it allows the achievement of the highest possible level of automation and reusability with minimum information collected in a very short period of time. In this methodology, we have prioritized quickness and cost saving sacrificing, to do so, the precision offered by other methodologies. In other words, the developed methodology has the aim of generating one of the best security configurations but not the optimal 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 that has been developed is a set of matrices that allow relating the different components of the ISMS (controls, assets, threats, vulnerabilities, risk criteria, procedures, registers, templates, technical instructions, rules and metrics) and that the model will use to generate automatically great part of the necessary information reducing noticeably the necessary time for the development and implementation of the ISMS. This set of interrelations between all the ISMS components allows 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 all times, we can have an updated valoration of how the security system of the enterprise evolves.

In this way and from the information obtained through the implementation in different enterprises, we have developed a methodology of information system security management and maturity and a model associated with it.

This methodology is composed of three main subprocesses:

- *GEGS – Generation of Schemas of Security Management.* The main objective of this subprocess is oriented to the construction of "schemas" that are necessary structures for ISMSs construction, created for a set of possible enterprises of the same category. These schemas are reusable and allow us to reduce the time of creation of the ISMS as well as its maintenance costs to make them adequate for SMEs dimension. The use of schemas is especially interesting in the case of SMEs because due to their special characteristics, they should have simple and very similar information systems.

  Within the follow-up of the security level of the controls at the maintenance stage of the ISMS, the interrelation between objects (see Figure 1) plays a fundamental role because thanks to the existing relations we can determine if the objects are affected by the unfulfilment of a rule or the incorrect use of a procedure in the ISMS, adequating their security level.

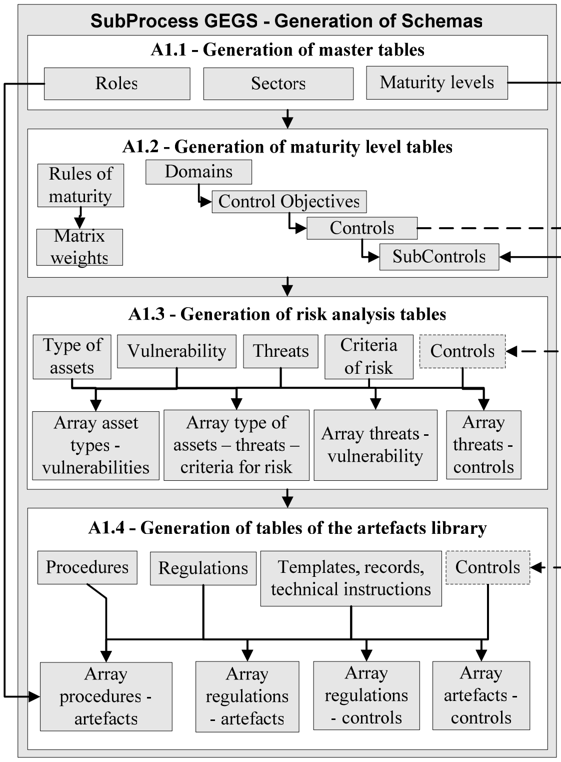

SubProcess GEGS - Generation of Schemas
A1.1 - Generation of master tables
Roles
Sectors
Maturity levels
A1.2 - Generation of maturity level tables
Rules of maturity
Domains
Control Objectives
Controls
Matrix weights
SubControls
A1.3 - Generation of risk analysis tables
Type of assets
Vulnerability
Threats
Criteria of risk
Controls
Array asset types - vulnerabilities
Array type of assets – threats – criteria for risk
Array threats - vulnerability
Array threats - controls
A1.4 - Generation of tables of the artefacts library
Procedures
Regulations
Templates, records, technical instructions
Controls
Array procedures - artefacts
Array regulations - artefacts
Array regulations - controls
Array artefacts - controls

Figure 1. Artefacts composing GECS subprocess

- *GSGS – Generation of Security Management Systems:* The main purpose of this subprocess is the creation of an ISMS appropriate for an enterprise, using, to do so, an existing schema (see Figure 2).

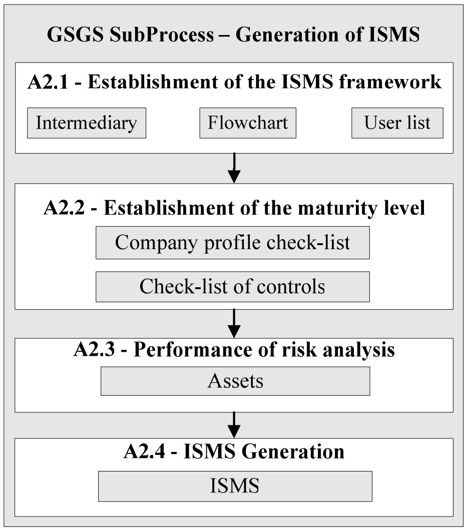

GSGS SubProcess – Generation of ISMS
A2.1 - Establishment of the ISMS framework
Intermediary
Flowchart
User list
A2.2 - Establishment of the maturity level
Company profile check-list
Check-list of controls
A2.3 - Performance of risk analysis
Assets
A2.4 - ISMS Generation
ISMS

Figure 2. Artefacts composing GSGS subprocess

- *MSGS –Maintenance of the Security Management System:* The main purpose of this subprocess is that of maintaining and managing the security of the enterprise information system providing updated information of a generated ISMS (see Figure 3).

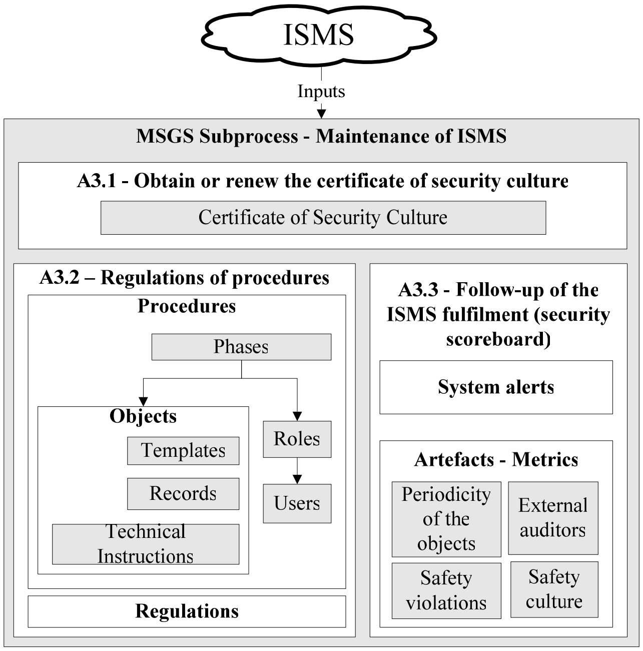

ISMS
Inputs
MSGS Subprocess - Maintenance of ISMS
A3.1 - Obtain or renew the certificate of security culture
Certificate of Security Culture
A3.2 – Regulations of procedures
Procedures
Phases
Objects
Templates
Records
Technical Instructions
Roles
Users
Regulations
A3.3 - Follow-up of the ISMS fulfilment (security scoreboard)
System alerts
Artefacts - Metrics
Periodicity of the objects
External auditors
Safety violations
Safety culture

Figure 3. Artefacts composing MSGS subprocess

Activity (A3.3) that manages the follow-up of the security level is centred in the third subprocess MSGS but it is supported by the structure of the schema and the interrelations established between the different objects of the ISMS for its functioning.

4. Scorecard for security management

The scorecard that has been implemented has the main objective of maintaining the maturity level of the ISMS updated as well as knowing at all times the level of fulfilment of the security controls composing the ISMS of the enterprise.

Now, we will describe the basic schema of inputs, tasks and outputs composing the activity in charge of managing this scorecard:

- *Inputs:* As inputs, we will: i) the certificate of security culture because, without it, we cannot access the information system of the enterprise; ii) input data of the users (e.g. measurements of the level of fulfilment of the controls by the security auditor as part of the recalibration process); iii) from the ISMS information repository, we will obtain information about changes in the level of fulfilment of the security controls.
- *Tasks:* The activity will be formed by seven tasks that are independent and that will be executed when necessary without a time limitation (represented by a clock in the schema). These tasks are as follows:
    - *T3.3.1 – Manage the security scorecard:* It allows the responsible for security (Cl/RS) to know at all times the level of security management of the information system without having to wait for expensive and late external audits.
    - *T3.3.2 – Manage the periodicity of the procedures:* It allows us to measure the impact of unfulfilling the execution of a procedure on the system.
    - *T3.3.3 – Manage the security violations:* It allows us to measure the impact that the unfulfilment of a security rule of one of the security regulations approved in the ISMS will have on the rest of artefacts forming the system.
    - *T3.3.4 – Manage the certificates of security culture:* It allows us to measure the level of the users with respect to the security culture of the enterprise in order to take corrective measures (e.g. Awareness or security courses).
    - *T3.3.5 – Perform periodic audits:* They will be performed periodically by an external auditor as a mechanism of recalibration of the scorecard.
    - *T3.3.6 – Perform general metrics:* It allows us to measure other ISMS specific factors associated with the functioning of procedures and controls ((e.g. response time to security incidents).
    - *T3.3.7 – Manage the alert system:* It facilitates that the responsible for security (Cl/RS) is informed of failures or distortions in the IS security management without having to supervise it continuously.
- *Outputs:* The output produced by this subprocess will consist of a series of reports associated with changes in the levels of fulfilment of the security controls and with violations of the regulations in order to make it possible that the security auditor (AuS) and the responsible for security (Cl/RS) can analyze it and determine improvements.

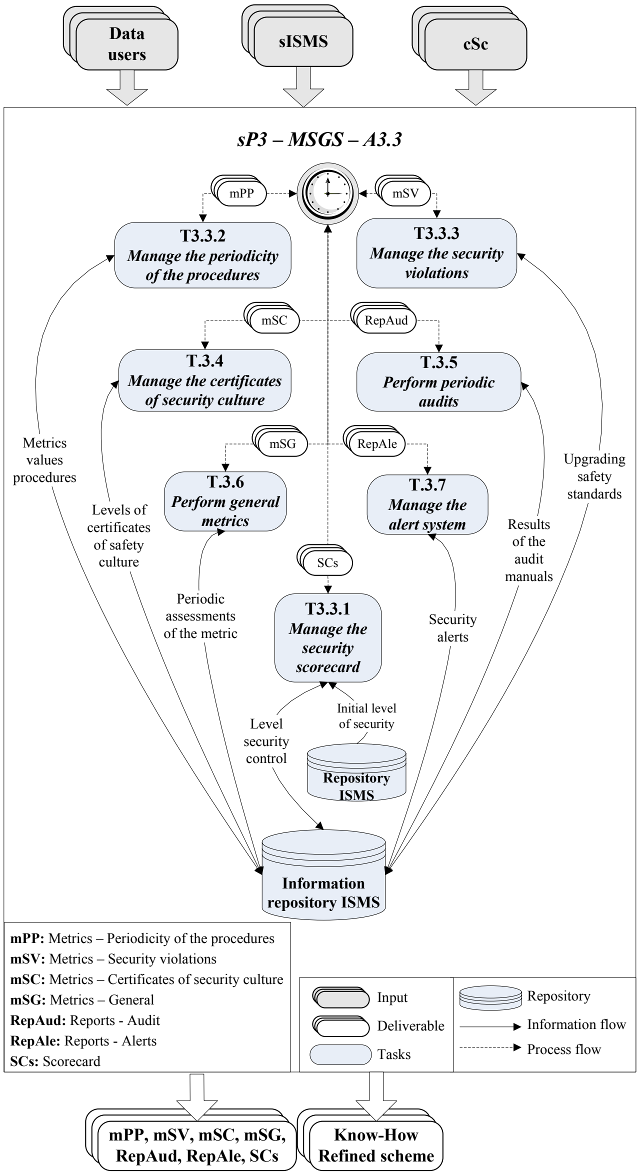

Data users
sISMS
cSc
sP3 – MSGS – A3.3
mPP
mSV
T3.3.2 Manage the periodicity of the procedures
T3.3.3 Manage the security violations
mSC
RepAud
T.3.4 Manage the certificates of security culture
T.3.5 Perform periodic audits
mSG
RepAle
Metrics values procedures
T.3.6 Perform general metrics
T.3.7 Manage the alert system
Upgrading safety standards
Levels of certificates of safety culture
Results of the audit manuals
SCs
Periodic assessments of the metric
T3.3.1 Manage the security scorecard
Security alerts
Level security control
Initial level of security
Repository ISMS
Information repository ISMS
mPP: Metrics – Periodicity of the procedures
mSV: Metrics – Security violations
mSC: Metrics – Certificates of security culture
mSG: Metrics – General
RepAud: Reports - Audit
RepAle: Reports - Alerts
SCs: Scorecard
Input
Deliverable
Tasks
Repository
Information flow
Process flow
mPP, mSV, mSC, mSG, RepAud, RepAle, SCs
Know-How Refined scheme

Figure 4. Detailed schema at the level of task of the activity A3.3

In Figure 4, the tasks that take part in the activity are shown in a much more detailed way and we can see how they interact with the ISMS repository that is in charge of containing the statistics and data introduced by the users of the information system during their daily work with the ISMS.

Each one of the tasks defined in this activity has a clearly defined objective to maintain the system updated that is:

Within these tasks, T3.3.2, T3.3.3, T3.3.4, T3.3.5 and T3.3.6 generate values that alter the security level of the enterprise represented in the scorecard (T3.3.1) and this can produce alerts in the system (T3.3.7). The functioning of the tasks of this system can be graphically seen in Figure 5.

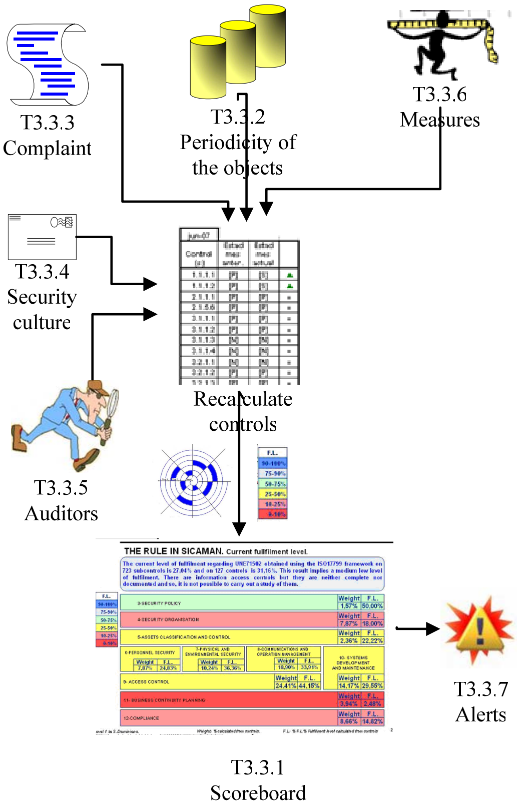


Figure 5. Graphical representation of the tasks of activity A3.3

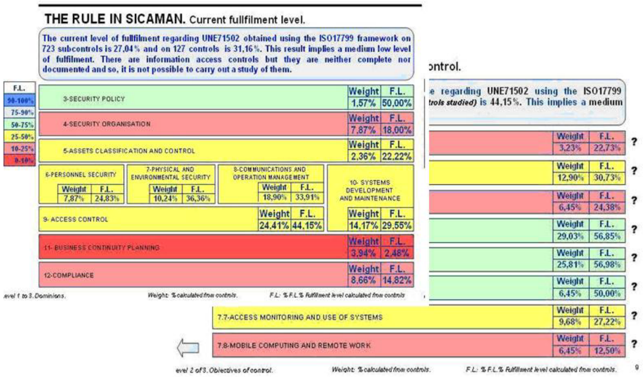
This activity has been designed to allow the ISMS to evolve the level of fulfilment of the security controls dynamically without the compulsory (but advisable) intervention of external auditors. Thus, the enterprise does not have to wait for the arrival of external auditors to know how the security of the information system is evolving because the system updates it continuously by changing the security level of the controls and readjusting all the objects of the system.

The result of each change is reflected in the level of fulfilment of the controls of the security scorecard that becomes the control center of the responsible for security (CI/RS) of the enterprise to analyze the evolution of the system and take corrective measures.

Within the activity in charge of maintaining the security level of the controls, a series of tasks to perform have been determined:

- *Task T3.3.1– Manage the scorecard of security controls:* The task has the purpose of performing updatings in the security controls composing the scorecard. The absence of this security scorecard in enterprises makes them not to have the ability of making decisions in the field of security at short term because they depend on the periodic visits of the auditors (approximately every two years) to be able to determine which controls have been generated as time goes by. However, in MGSM–PYME methodology, the existence of a dynamic security scorecard makes it possible that the responsible for security (CI/RS) knows at all times which security controls require to be more supervised and over which controls corrective measures must be taken.

In Figure 6, we can see an example of different levels of the security scorecard.


THE RULE IN SICAMAN. Current fullfilment level.

The current level of fullfilment regarding UNE71502 obtained using the ISO17799 framework on 723 subcontrols is 27,04% and on 127 controls is 31,16%. This result implies a medium low level of fulfilment. There are information access controls but they are neither complete nor documented and so, it is not possible to carry out a study of them.

F.L.
90-100%
75-90%
50-75%
25-50%
10-25%
0-10%

	Weight	F.L.
3-SECURITY POLICY	1,57%	50,00%
4-SECURITY ORGANISATION	7,87%	18,00%
5-ASSETS CLASSIFICATION AND CONTROL	2,36%	22,22%
6-PERSONNEL SECURITY	7,87%	24,83%
7-PHYSICAL AND ENVIRONMENTAL SECURITY	10,24%	36,36%
8-COMMUNICATIONS AND OPERATION MANAGEMENT	18,90%	33,91%
9- ACCESS CONTROL	24,41%	44,15%
10- SYSTEMS DEVELOPMENT AND MAINTENANCE	14,17%	29,55%
11- BUSINESS CONTINUITY PLANNING	3,94%	2,48%
12-COMPLIANCE	8,66%	14,82%

evel 1 to 3. Dominions. Weight: % calculated from controls. F.L.: % F.L.% Fulfilment level calculated from controls

ontrol.

e regarding UNE71502 using the ISO17799 trols studied) is 44,15%. This implies a medium

	Weight	F.L.	
	3,23%	22,73%	?
	12,90%	30,73%	?
	6,45%	24,38%	?
	29,03%	56,85%	?
	25,81%	56,98%	?
	6,45%	50,00%	?
7.7-ACCESS MONITORING AND USE OF SYSTEMS	9,68%	27,22%	?
7.8-MOBILE COMPUTING AND REMOTE WORK	6,45%	12,50%	?

evel 2 of 3. Objectives of control. Weight: % calculated from controls. F.L.: % F.L.% Fulfilment level calculated from controls. 9

Figure 6. Levels of the security scorecard.

Task T3.3.2– Manage the periodicity of procedures: The task shows one of the specific metrics of the methodology whose objective is to provide each procedure with an execution periodicity (minimum time for the procedure to be executed). In this way, when one of the ISMS procedures is not executed within this period of time, this task generates an alert whose objective is to reduce the security level of the controls associated with this ISMS procedure and the elements associated with it. The responsible for security (CI/RS) will finally determine if reducing security makes sense or not. On the contrary, when a procedure is executed before the established periodicity, the level of fulfilment of the associated controls will increase.

The periodicity system of the objects has been planned to be autoregulated every year. For that reason, at the beginning, we establish that all objects have a monthly periodicity (e.g. if the first year a procedure is executed 50 times, the following year, the periodicity of such procedure would be 365/50, in other words, weekly and the following year, we will calculate the average taking into account all the information of the database related to the periodicity of the object to obtain the periodicity that is closer to reality. On the contrary, if a procedure must be executed only twice a year, initially the alert will appear each month and the responsible for security will determine if the procedure is actually being unfulfilled. If so, he/she will approve a penalization (–1%), or on the contrary, if it has not been necessary to execute the procedure, he/she will cancel the penalization.

Thus, periodically, each procedure tries to make the responsible for security (CI/RS) aware of its existence regulating the level of fulfilment of the associated controls.

- *Task T3.3.3 Manage the security violations:* The objective is that of providing other measurement mechanism that allows us to have the level of security management of the enterprise updated. This task lets us control the violations of the security regulations of the ISMS of the enterprise, penalizing the controls associated with the rules that have been violated, always when the responsible for security (Cl/RS) considers that there has been a violation.

Opposite to the autoregulation mechanisms included in other tasks, the percentage of penalization in the system of complaint is high because there is an evidence of a violation of the security regulations. In our methodology, we have established a penalization of 1% over the total value of the security controls related to the unfulfilled regulation and the loose of one point in the certificate of security culture of the user of the information system that has caused the violation.

This task has only a penalization character because it does not provide a mechanism that allows the increase of the level of fulfilment of the controls or of the certificate of security culture.

At last, we have determined not to reward the user that makes the report to avoid that this report becomes invalidated for that.

- *Task T3.3.4 – Manage the certificates of security culture:* The purpose is to update the score of the certificates of security culture as well as that of the security controls associated with them when certain actions take place: i) violations of the security regulations; and ii) when the certificate of security culture is lost because of not having the required points.

Throughout the research, we have determined that the higher is the security culture of the enterprise, the higher is the number of reports that come from the users; even more when such reports currently do not imply serious penalizations to those users reported.

When a report of a security incidence is made and the responsible for security considers that the report is justified and approved it; this fact affects not only the global security level of the enterprise but also the score of the certificate of security culture of the user that performed the security violation. Each security violation implies the loose of one point in the certificate of security culture (NCS) that the user had at that moment and that was the result of the mark obtained in the security culture test minus the points already lost during the validity period of that certificate because of violations of the regulations in force in the enterprise. If the loose of points due to security violations makes the score of the certificate of security culture be lower than 5 points, the user will loose the certificate as well as the access to the information system of the enterprise until he/she passes the test again and obtains a new certificate of security. All this process can be seen in Figure 7.

This process is used as a preventive control for users of the information system to be conscious of the cost that violations of regulations imply. Furthermore, the measure is not excessively serious and therefore, the users do not reject it. This control does not imply a management cost either of time or of resources representative for the enterprise but it does imply an important effort to establish a correct security culture of the enterprise.

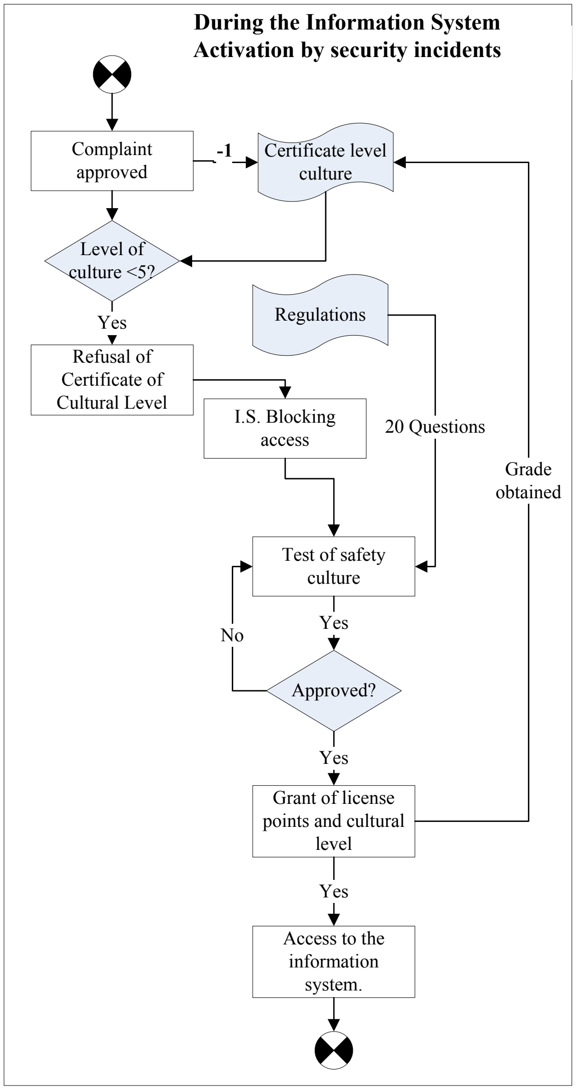

During the Information System Activation by security incidents
Complaint approved
-1
Certificate level culture
Level of culture <5?
Yes
Regulations
Refusal of Certificate of Cultural Level
I.S. Blocking access
20 Questions
Grade obtained
Test of safety culture
No
Yes
Approved?
Yes
Grant of license points and cultural level
Yes
Access to the information system.

Figure 7. Alteration of the NCS due to a violation of the regulations

In Figure 8, we can see how the scores of the security culture test are related to the regulations-controls matrix in a way that when a security certificate is obtained with a low mark, this affects the controls associated with the regulations from which the questions have been obtained because when the user fails a question of the test, the percentage of the level of the controls associated with such question decreases in a (–0.1%). In the same way, if the answer is correct, the level of the controls increases in a (+0.1%).

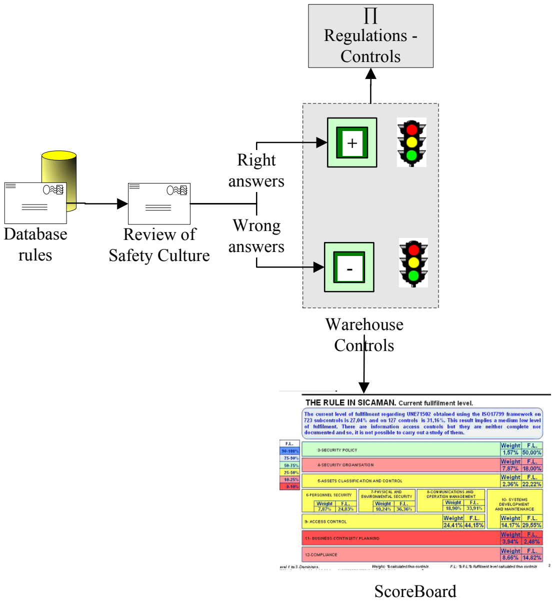


Figure 8. Manage the certificates of security culture.

- *Task T3.3.5 – Performance of periodic audits:* The objective is the performance of external audits that will be used for recalibrating the levels of fulfilment of the security controls composing the ISMS scorecard.

This task consists of the performance of a verification list (that could be the one performed in task T1.2.2) by the security auditor (AuS) and comparing the result of the level of fulfilment obtained for every ISMS security control in the evaluation of the external security auditor (AuS) to the current level of fulfilment of the scorecard with the objective of:. i) determining the variations existing between the controls and their reasons as well as determining which metrics have worked incorrectly; y ii) recalibrating the scorecard, updating again the level of fulfilment of the security controls.

Our methodology has been put forward to reduce the need of periodic audit due to two reasons: i) The first one is that they imply a huge cost for the enterprise; and y ii) the second one is that as they are performed in long periods of time (e.g. every two years), they cannot be used to take measures at short term that are the ones that really mean a cost saving for the Enterprise because they maintain the security level.

Throughout the research, we have come to the conclusion that if the responsible for security detects the degeneration of a security control at an early stage, it is very easy to determine and apply corrective measures because the control is only suffering a degeneration but it still has the pillars over corrective measures must be applied. On the contrary, if a level starts to degenerate and this procedure takes long time without taking corrective measures, finally, the control looses all its consistency and to fulfil it again an enormous effort will be required. This is due to the fact that when a control is degradated during a long period of time, finally it will negatively affect the security culture of the Enterprise. Therefore, our methodology tries to avoid to depend only on the periodic audits (e.g. every two years) leaving them just as an autoregulation mechanism to determine small deviations that could have arisen.

The results of the audit concerning the level of fulfilment of the security controls should not differ in more than a 5% of the current level of fulfilment of the ISMS scorecard. If they did, we should determine the reasons of the deviations: i) malfunctioning of the defined metrics; ii) lack of metrics; iii) incorrect use of the ISMS by the users; iv) lack of supervision of the responsible for security (CI/RS), v) etc.

- *Task T3.3.6 – Manage the general metrics:* The objective is that of providing new information about the state of the security of the ISMS through the use of a series of general metrics.

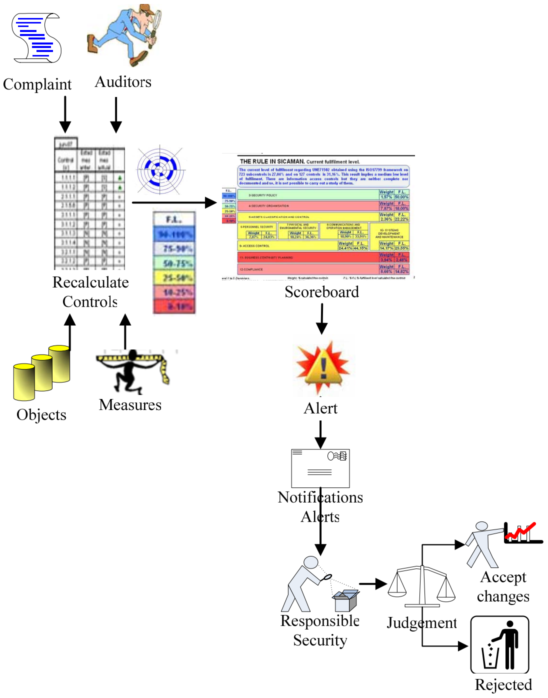


Figure 9. Alert system for security levels control

These metrics do not affect the level of fulfilment of the ISMS controls directly but provide the responsible for security (CI/RS) with information about measures that must be taken to improve the information system security Management.

The responsible for security (CI/RS) can decide to alter the value of the levels of fulfilment of the security controls manually from the information provided by these metrics, if he/she considers it appropriate.

- *Task T3.3.7 – Manage the alert system:* The objective is that of avoiding that the responsible for security (CI/RS) has to be continuously analyzing all controls of the security scorecard to determine if a degeneration of the system is taking place.

This task sends an alert to the responsible for security (Cl/RS) when the level of fulfilment of a control is higher than one of the established limits (eg. 0–10%, 10–25%, 25–50%, 50–75%, 75–90%, 90–100%) indicating that a change from the limit X to the limit Y has occurred and the reasons that have caused this change. Thus, the responsible for security (CI/RS) can determine if the reasons have been objective or if we are dealing with a bad interpretation of the system and in such a case, he/she can regulate again the control level. In Figure 9, we can see graphically the flow followed by the task.

5. Conclusions

In this paper, we have presented a model that allows us to know at all times the level of fulfilment of the different controls forming the ISMS of a SME through the use of a scorecard and a set of metrics. We have defined how we can use this model and the improvements that it offers, focusing on its main improvement: the possibility of knowing at all times the level of security of the controls composing the security Management system and if these controls are being degradated in a way that the responsible for security can make decisions at short term that avoid a greater degradation of the security controls.

The characteristics offered by the model and its orientation towards SMEs have been received very well and its application is being very positive because it allows this kind of enterprises to access the use of scorecards within the information security Management Systems. So far, this had been only possible for big enterprises. Moreover, with this model, we obtain short-term results and we reduce the costs implied by the use of other methodologies or the application of corrective measures at long term, thus achieving a greater degree of satisfaction of the Enterprise.

At last, we consider that the work carried out must be widened with new specifications and new metrics that allow us to obtain more precise results in the scorecard.

All future improvements of the scorecard are being oriented to improve its precision but always respecting the principle of resource cost s in other words, we look for improving the precision offered by the ISMS but without incurring in greater costs of generation and maintenance of the ISMS.

6. ACKNOWLEDGMENTS

This research is part of the following projects: BUSINESS (PET2008-0136) granted by the “Ministerio de Ciencia e Innovación” (Spain), QUASIMODO (PAC08-0157-0668) project financed by the “Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha”, SISTEMAS (PII2I09-0150-3135) project financed by the “Consejería de Educación y Ciencia 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).

7. REFERENCES

[1] Wiander, T. Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.

[2] 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.

[3] 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.

[4] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.

[5] Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.

[6] 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.

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

[8] ISO/IEC27004, ISO/IEC FCD 27004, Information Technology - Security Techniques - Information Security Metrics and Measurement (under development). 2009.

[9] ITILv3.0, ITIL, Information Technology Infrastructure Library., C.C.a.T.A. (CCTA). Editor. 2007.

[10] COBITv4.0, Cobit Guidelines, Information Security Audit and Control Association. 2006.

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