future internet

MDPI

Article

Applying the Action-Research Method to Develop a Methodology to Reduce the Installation and Maintenance Times of Information Security Management Systems †

Antonio Santos-Olmo [1,2], Luis Enrique Sánchez [2,3,*], David G. Rosado [2], Eduardo Fernández-Medina [2] and Mario Piattini [4]

1 Research and Development Department, Sicaman Nuevas Tecnologías, Tomelloso 13700, Spain; asolmo@sicaman-nt.com
2 Research Group GSyA, University of Castilla-la Mancha, Ciudad Real 13700, Spain; david.grosado@uclm.es (D.G.R.); eduardo.fdezmedina@uclm.es (E.F.-M.)
3 Project Prometeo of Senescyt, University of the Armed Forces (ESPE), SanGolqui 170501, Ecuador
4 Research Group Alarcos, University of Castilla-la Mancha (UCLM), Ciudad Real 13700, Spain; mario.piattini@uclm.es
* Correspondence: luisenrique@sanchezcrespo.org; Tel.: +34-926-502-545
† This paper is an extended version of paper published in the VIII Congreso Iberoamericano de Seguridad Informática—CIBSI, Quito, Ecuador, 10–12 November 2015.

Academic Editor: Luis Javier Garcia Villalba
Received: 12 February 2016; Accepted: 8 July 2016; Published: 22 July 2016

Abstract: Society is increasingly dependent on Information Security Management Systems (ISMS), and having these kind of systems has become vital for the development of Small and Medium-Sized Enterprises (SMEs). However, these companies require ISMS that have been adapted to their special features and have been optimized as regards the resources needed to deploy and maintain them, with very low costs and short implementation periods. This paper discusses the different cycles carried out using the 'Action Research (AR)' method, which have allowed the development of a security management methodology for SMEs that is able to automate processes and reduce the implementation time of the ISMS.

Keywords: cybersecurity; Information Security Management Systems; ISMS; Action Research; process improvement; cost saving; time reduction; SMEs; ISO27001; ISO27002

1. Introduction

Companies in the globalised competitive business environment are increasingly more dependent on information systems, since they have proved to have an enormous influence as regards raising their level of competitiveness [1]. However, if these information systems do not have appropriate security management, then they have no real value since they cannot provide companies with sufficient guarantees of continuity [2,3]. Companies are therefore becoming conscious of just how important appropriate information security systems and their correct management really are [4]. This signifies that although many businesses take the risk of doing without adequate protection, many others have understood that information systems are useless without security management systems and their associated protection measures.

Security has existed in the world of computing for more than 30 years [5,6], but although a multitude of globally accepted security solutions has come into being (e.g., the subject/object access matrix model [7], access control lists [8], multilevel information flow security [9], public key

cryptology [10,11] or the role-based access control model [12], to name but a few), the millions of users connected by networks are still generally highly mistrustful of their security.

An Information Security Management System (ISMS) can be defined as a management system that is used to establish and maintain a secure environment for information. The principal objective of ISMSs is to tackle the putting into practice and maintenance of the processes and procedures needed to manage the security of information technologies [1,4,13–15]. Dhillon [16] states that ISMSs are concerned not only with the security of information but also include the management of that information's formal and informal aspects [3]. These actions include the identification of the information's security needs and the putting into practice of strategies to satisfy those needs, measure results, and improve protection strategies [2,6].

At the present time, which is considered to be the era of the Internet, security has become a generalised and increasing concern in all areas of society: business, domestic, financial, individual, etc. [17]. Society increasingly depends on a wide range of critical mission software systems, such as air traffic control systems, financial systems, or public health systems. Given the potential losses that those companies that trust in these hardware and software systems may have to confront, it is critical to appropriately ensure the security of information systems from the beginning of their lifecycles [18,19]. The author of [20], moreover, analysed the SMEs in Europe and the United States, and reached the conclusion that the Internet has led to a series of changes within the framework of global collaboration. This makes it necessary for these companies to protect their information systems, which are becoming the neural centre of their growth and changing the way in which they communicate, do business, and attain objectives. All of this has led to an increase in delinquency and threats to security, such as spam, phishing, and viruses, thus destroying users' confidence in the Internet [21].

The information security problem is characterised by its complexity and interdependence. Security management consists of several important factors and elements that are interrelated. This situation is complicated further still by the human factor, since human beings have free will and always act in their own interests [22]. Furthermore, the fact that most business activities are beginning to depend on the Internet makes security one of the principal concerns as regards creating a sustainable business fabric [23]. The SMEs in developed countries tend to have a weak understanding of information security, security technology, and control measures, and tend to forget about risk analyses or the development of security policies [24–27]. This is possibly owing to the fact that SMEs lack the resources, time, and specialised knowledge needed to coordinate information security or provide their employees with appropriate education or training in information security [24,25,28]. A very different explanation can, however, be found in the literature. Gupta and Hammond [25] and Johnson and Kock [29] point out that, since SMEs lack a specialised knowledge of security technologies, they tend to maintain their security using the technologies with which they are already familiar. Moreover, SMEs do not view security as being linked with their business strategies, although it has a direct impact on their fulfilment of those strategies [30]. In fact, recent research shows the need to link information security with strategic planning information systems, and therefore with the company's objectives [31].

The installation and long-term maintenance of information security management systems must, therefore, cost little if they are to be used by small businesses.

In order to obtain a low-cost methodology for the installation of these systems, it is first necessary to determine why businesses really discontinue their use. The ideal manner in which to do this is by means of what is denominated as the 'Action-Research' method.

We therefore decided to begin continuously applying this research method while dealing with consultations regarding ISMS from customers at the Sicaman Nuevas Tecnologías S.L. Company. The objective of this was to obtain a process that would gradually become more and more refined and that would allow quality installation and maintenance, but at a low cost.

This paper continues in Section 2, in which the research method used, the existing security methodologies and models, and their current tendency in the case of SMEs are described. A general view of the methodology developed is provided in Section 3, while a description of how the research

environment and the users of the test were determined is given in Section 4. Section 5 gives an analysis of the process followed to obtain the methodology by means of applying the Action Research (AR) method, and the paper concludes in Section 6, in which we provide our conclusions and indicate our future work.

2. State of the Art

2.1. The Action Research Method

Qualitative research methods, and particularly, Action Research, have in recent years attracted the attention and gained the acceptance of the scientific community related to information systems [32–34].

Action Research does not refer to a specific research method but rather to a class of methods that have the following in common: (i) orientation towards action and change; (ii) focus on a problem; (iii) an 'organic' modelling process that encompasses systematic and sometimes iterative steps and, and (iv) collaboration among participants.

The term 'action research' was first coined by Kurt Lewin in 1946 in his work entitled 'Action research and minority problems'. The AR method is characterised as being comparative research into the conditions and effects of various types of research and social action, in which the most prominent aspect is social action using a spiral process consisting of several steps, each of which is composed of various cycles: planning, action, and the search for facts regarding the results of the action [32,33].

The application of this method is directly related to the objective pursued in this research: defining a methodology and a security management model for SMEs.

The research has been carried out by applying the action-research method in its participant variant, i.e., that in which the critical reference group puts the recommendations made by the researcher into practice, and shares the effects and results with that researcher. The following participants were therefore defined:

- *The researcher*, which is in this case the GSyA Research Group, made up of professors at the School of Computer Sciences at the University of Castilla-La Mancha in Ciudad Real, Spain.
- *The object being researched*, i.e., the problem to be resolved, which is in this case improving the security management of information technologies.
- *The critical reference group (CRG)*: those for whom the research is being carried out and who also participate in the research. This consists of the Sicaman Nuevas Tecnologías S.L. (SNT) company, its customers, and the participants in the research projects.
- *The fourth participant – the beneficiary*, which consists of those organisations that may benefit from the results of the work, i.e., all those small and medium-sized companies that might wish to apply advanced information security management methods to their information systems in order to improve the security of their information technology products and processes in a controlled and methodical manner. The results obtained after carting out this research will improve the efficiency of the installation and maintenance processes of information security management systems. The principal beneficiaries will therefore be all those companies that are linked to the critical reference group.

The stages identified in order to demonstrate the cyclical nature of action research have been applied in this research as follows:

- *Planning:* Once the problem related to incorporation of security management systems into SMEs had been identified, we planned the development of a methodology that would allow the creation of an ISMS with the minimum number of resources, which would be adapted to the size and maturity of the company.
- *Action*: having defined the principal elements involved in the ISMS-creation process, we then went on to create a model and to apply it in determined case studies. The elements that would be used to construct the final ISMS were also applied in the case study.

- *Observation*: Once the elements had been applied and the ISMS had been created, the results obtained were evaluated. This allowed us to improve the original proposals and to eventually define a methodology that would systemise the creation and evolution of an ISMS for a company, along with a model that would permit its validation. The entire method is supported by a prototype that allows the simple generation of ISMSs and the work to be carried out with them in order to analyse their evolution over time.
- *Reflection:* the cyclical nature of the action research method was borne in mind, and results that were the product of successive iterations were therefore obtained. The research team has shared and contrasted these results in national and international forums related to the topics being dealt with in this research.

A schema of the participants and the cycles resulting from the application of the action research method in this research is shown in Figure 1.

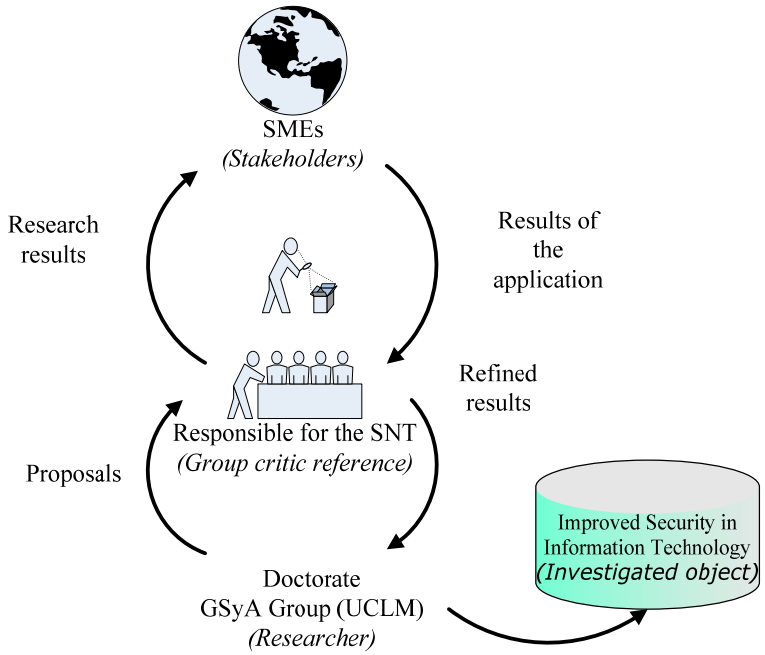

Figure 1. Application of Action Research during research.

2.2. Security Management in SMEs

A large number of information security processes, frameworks, and methods whose intention is to reduce the lacks shown in the Introduction and to lessen the losses that they cause have appeared, and the need for their implementation is being increasingly recognised by organisations. However, as shown previously, they are inefficient in the case of SMEs [35,36].

With regards to the most prominent standards, it is possible to state that the majority of security management models are based on the ISO/IEC27001 [37] and ISO/IEC27002 [38] international standards, and that the security management models that are proving to be most successful at large companies are ISO/IEC27001 [37], COBIT [39], and ISM3, but they are difficult to install and require an investment that is too high for the majority of SMEs to be able to assume [25,35]. Although some very interesting new proposals oriented towards this type of companies are appearing, the way in which they confront the problems is incomplete.

Numerous bibliographical sources detect and highlight how difficult it is for SMEs to use traditional security management maturity methodologies and models, since they have been conceived for large businesses [40–43]. It has repeatedly been justified that the application of this type of maturity

models and methodologies is difficult and costly for SMEs. Moreover, even large organisations tend to adopt related groups of processes as a set, rather than dealing with processes independently [44].

The aforementioned security management methodologies and models have not proved to be valid in SMEs for three reasons [40–44]:

- They were developed by bearing in mind organisations that have far more resources.
- They deal with only part of the security management system, and almost none of them confront the installation of these systems from a global perspective, which obliges companies to acquire, implement, manage, and maintain various methodologies, models, and tools in order to manage security. What is more, the few applications that have attempted to tackle all the aspects of security management are expensive to acquire and require a complex management and costly maintenance, signifying that they are not appropriate for SMEs.
- Finally, it is possible to conclude that, although several standards, regulations, guidelines to good practices, security management, and risk analysis methodologies and models exist, they are not integrated into a global model that can be applied to small and medium-sized companies with guarantees of success.

Therefore, and as a conclusion to this section, it could be said that tackling the problem of developing a new methodology for security management and its maturity for SMEs' information systems is both pertinent and opportune, as is the development of a model that will validate its functioning and a tool that will support this model, based on the problems that this type of company confronts—which have led to continuous failures when these systems are installed in this type of company.

3. The MARISMA Framework

When we embarked upon our research, there were no methodologies that could clearly be used to apply 'Security Management Plans' in companies. There were only standards, such as the BS799 or COBIT, which explained 'what to do' but not 'how to do it'. In order to confront the aforementioned challenge, we therefore decided to develop a methodology for ISMSs that would provide a solution to the problems detected, denominated as MARISMA (Metodology for Risk Analysis and Information Security MAnagement).

The MARISMA methodology was created in such a way that it would be valid for any organisation, regardless of its size, but it was validated in and oriented towards SMEs, since these companies are far more dependent on low-cost systems. What is more, SMEs have the highest rate of failure as regards the installation of these security management methodologies [45,46], and it was therefore important to ensure that the new methodology would be valid for them, but without the loss of quality and scientific rigour required by this type of systems.

One of the objectives pursued by the MARISMA methodology is that of it being simple to apply, and that the model developed over it will allow the greatest possible level of automation and reusability to be obtained with the minimum amount of information, gathered in a very small amount of time. Speed and cost-saving have been made a priority in this methodology, signifying that the precision offered by other methodologies has been sacrificed. That is to say, the methodology developed seeks to generate one of the best security configurations, although not necessarily that which is optimum, with priority being given to time and cost saving rather than precision, although guaranteeing that the results obtained are of a sufficiently high quality.

In this way, and through the use of the information obtained after implementation at various companies, we have developed an information security system management and maturity methodology and its associated model (see Figure 2).

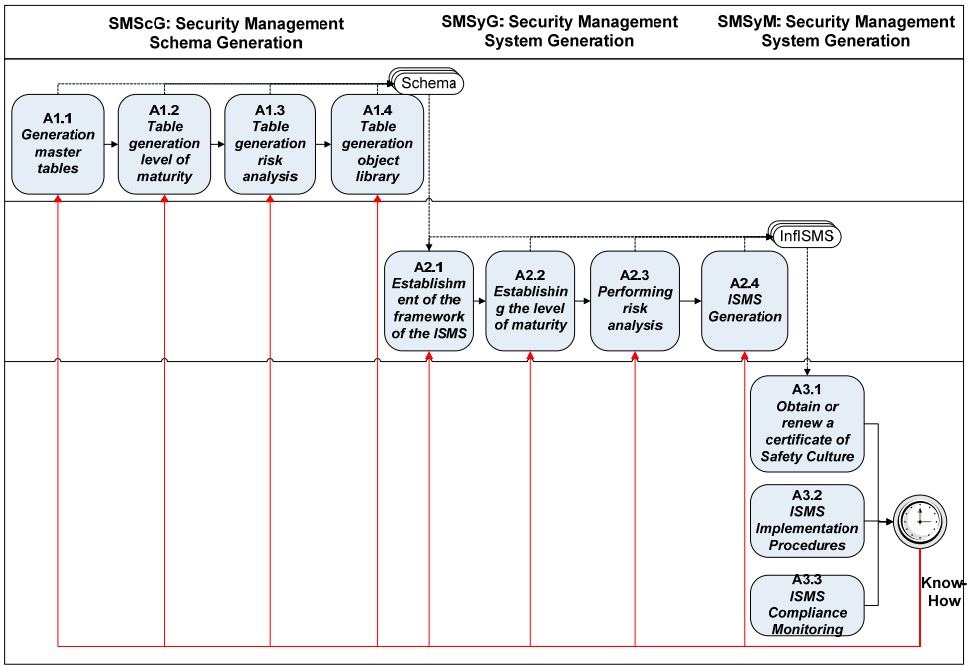

Figure 2. Sub-processes of the methodology.

This methodology consists of three principal sub-processes:

- *SMScG—Security Management Scheme Generation*: The principal objective of this sub-process is the construction of 'schemas', which are the structures needed to build ISMSs, and which are created for a possible set of companies in the same category. These schemas are reusable and allow the time needed to create the ISMS to be reduced, along with its maintenance costs, thus making them suitable for the dimension of an SME [45]. The use of schemas is of particular interest in the case of SMEs since their special characteristics signify that they tend to have simple information systems that are very similar to each other. This sub-process is formed of the following activities and tasks:
    - *Activity A1.1—Generating master tables:* T1.1.1—Establishing the roles in the schema, T1.1.2—Establishing the business sectors, T1.1.3: Establishing the maturity levels.
    - *Activity A1.2—Generating maturity level tables:* T1.2.1—Establishing maturity rules, T1.2.2—Establishing controls.
    - *Activity A1.3—Generating risk analysis tables:* T1.3.1—Selecting types of assets, T1.3.2—Selecting threats, T1.3.3—Selecting vulnerabilities, T1.3.4—Selecting risk criteria, T1.3.5—Establishing relationships between types of assets and vulnerabilities, T1.3.6—Establishing relationships between threats and vulnerabilities, T1.3.7—Establishing relationships between threats and controls, T1.3.8—Establishing relationships among types of assets, vulnerabilities and risk criteria.
    - *Activity A1.4—Generating artefact library tables:* T1.4.1—Selecting rules, T1.4.2—Selecting procedures, T1.4.3—Selecting registers, T1.4.4—Selecting templates, T1.4.5—Selecting technical instructions, T1.4.6—Selecting metrics, T1.4.7—Establishing relationships between rules and artefacts, T1.4.8—Establishing relationships between rules and controls, T1.4.9—Establishing relationships between artefacts and controls, T1.4.10—Establishing relationships between procedures and artefacts.
- *SMSyG—Security Management System Generation*: The principal objective of this sub-process is the creation of an ISMS that is appropriate for a company by using an already-existing schema.

- *Activity A2.1—Establishing the framework of the ISMS:* T2.1.1—Requesting the valid interlocutor, T2.1.2—Requesting the company's organigram, T2.1.3—Obtaining the list of information system users and their roles.
- *Activity A2.2—Establishing the maturity level:* T2.2.1—Gathering business information, T2.2.2—Gathering technical information from the information system, T2.2.3—Obtaining the security maturity level.
- *Activity A2.3—Carrying out the risk analysis:* T2.3.1—Identifying assets, T2.3.2—Generating the risk matrix and the improvement plan.
- *Activity A2.4—Generation of the ISMS:* T2.4.1—Generation of ISMS objects, T2.4.2—Presentation of results to interlocutor.

- *SMSyM—Security Management System Maintenance*: The principal objective of this sub-process is to maintain and manage the security of the company's information system, providing information that is updated in the time of an ISMS generated.

  - *Activity A3.1—Obtaining and renewing safety culture certificate:* T3.1.1—Taking safety culture test.
  - *Activity A3.2—Executing ISMS procedures:* T3.2.1—Activate general procedure, T3.2.2—Activate report procedure.
  - *Activity A3.3—Following up the fulfilment of the ISMS:* T3.3.1—Managing security scorecard, T3.3.2—Managing periodicity of procedures, T3.3.3—Managing security violations, T3.3.4—Managing safety culture certificates, T3.3.5—Realisation of periodical audits, T3.3.6—Realisation of general metrics, T3.3.7—Managing the alarm system.

The process followed to obtain the various activities and tasks of which the MARISMA methodology is composed is analysed in the following section. This is done by using the action research method and adapting it to the characteristics of SMEs [47,48].

4. The Research Environment

In order to apply the Action-Research method, we decided:

- To do so with the Sicaman Nuevas Tecnologías S.L. company's customers in the case of ISO27001. This company was created in 1998, and one of its strategic divisions was focused on the installation of ISMSs. In 1999, the company began to implement 'Security Management Plans' under the BS7799 standard, and it then went on to use the UNE71502 regulation and the 17799 standard, and finally the ISO27001 standard. Tremendous faults were detected in the system from the outset, along with a low acceptance rate by customers, for whom it provided few benefits.
- To solicit help from the researchers from the Alarcos and GSyA group at the University College of Computer Science at the University of Castilla-La Mancha in order to establish a coherent and progressive methodology that would allow us to identify the faults and the reasons why the 'Security Management Plans' were not obtaining the desired results.
- To select a sample of 10 Spanish companies from the autonomous regions of Castilla-La Mancha and Madrid that were related to ICT, had between 10 and 50 employees (SMEs) and would be interested in installing ISMSs. The size of the companies was limited, since if they were too small (<10 employees) they would not have the minimum resources required to carry out the research, and also because they are unstable as regards changes in the market. Companies with more than 50 employees were not, meanwhile, considered because they tend to have adequate economic resources and do not, therefore, have a great need for low-cost systems.
- Initially we did not determine the duration of the research, although we estimated that it would take between five and 10 years to obtain an appropriate model. The research process eventually

began in June 2005, under the UNE71502 standard, and was completed in June 2015 under the ISO27001:2013 standard.

- This research was co-financed from the outset, and continues to be so. The principal projects involved in this research are shown as follows:

  - DIMENSIONS—Design and Measurement of Safe Information Systems. Code: PBC-05-012-1. Financing entity: the Autonomous Community of Castilla-La Mancha and FEDER. Participating entities: the University of Castilla-La Mancha, the University of Alicante and the University of Murcia. Duration: 1 January 2005–31 December 2007.
  - MÍSTICO—Definition of a Security Model Integrated into Information and Communication Technologies. Financing entity: FEDER and the Education and Science Council of the Autonomous Community of Castilla-La Mancha. Participating entities: the University of Castilla-La Mancha, the University of Málaga and SICAMAN-NT. Duration: 1 January 2006–31 December 2008.
  - SCMM-PYME—Security Maturity Model for Small and Medium-Sized Enterprises. Code: FIT-360000-2006-73. Financing entity: the Ministry of Industry, Tourism and Commerce. Participating entities: Sicaman Nuevas Tecnologías and the University of Castilla-La Mancha. Duration: 1 January 2006–31 December 2007.
  - Thematic Research Network in the field of Security and Confidence for Information Systems in a Connected Society (TIN2006-26885-E). Financing entity: the Ministry of Education and Science. Participating entities: Ciudad Real City Council, European Experts in Computer Science, Sicaman Nuevas Tecnologías, University of Alicante, University of Castilla-La Mancha, Catholic University of Maule (Chile), Polytechnic University of Catalonia, University of Deusto, University of Málaga, University of Murcia, University of Rey Juan Carlos, University of Seville and University of BioBio. Duration: 1 October 2006–1 October 2007.
  - SEGMENT—Security for SMEs: Integral Management and Measurement (HITO-09-138). Financing entity: The Education and Science Council of the Autonomous Community of Castilla-La Mancha. Participating entities: the University of Castilla-La Mancha and Sicaman Nuevas Tecnologías. Duration: 1 September 2009–1 September 2010.
  - MARISMA—Metodology for Risk Analysis and Information Security MAnagement (HITO-2010-28). Financing entity: the Education and Science Council of the Autonomous Community of Castilla-La Mancha. Participating entities: Collaboration agreement between the University of Castilla-La Mancha and Sicaman Nuevas Tecnologías. Duration: 1 September 2010–1 September 2011.
  - SIGMA_CC—Security Governance and Safe Migration of Computation Systems in the Cloud (TIN2012-36904). Financing entity: the Ministry of Economy and Competitiveness. Participating entities: the University of Castilla-La Mancha. Duration: 1 September 2012–30 September 2015.
  - W2B—Commercial Innovation Project for SAAS Services (1313REDA125). Financing entity: the Autonomous Community of Castilla-La Mancha. Participating entities: Sicaman Nuevas Tecnologías. Line: innoempresa. Duration: October 2013–October 2014.
  - Computational Platforms for Entertainment, Experimentation, Management and The Mitigation of Attacks against Cyber-Security (2015-PIC-019). Financing entity: the University of the Armed Forces (ESPE—Ecuador). Participating entities: the University of the Armed Forces (ESPE) and the National Network of Research and Education of Ecuador—CEDIA. Line: Research projects. Duration: 1 January 2015–31 December 2016.
  - ERABAC—Risk Analysis and Valuation of Information Assets in the Cloud (1315ITA227). Financing entity: M.D. of Companies, Competitiveness and Internationalisation of the Council for Economy, Businesses and Employment of the Autonomous Community of

Castilla-La Mancha. Participating entities: Sicaman Nuevas Tecnologías. Line: Business Innovation Support in Castilla-la Mancha. Duration: November 2015–November 2016.

5. Applying the Action-Research Method

This section is divided into five sub-sections, in the first of which we provide a summary of the principal lessons learnt during the application of the Action-Research method during the installation phase. In the second sub-section we analyse the main conclusions reached during this phase, while in the third we analyse the improvement cycles in the maintenance phase. In the fourth sub-section we analyse the principal conclusions reached during this part of the research. Finally, in the fifth sub-section we analyse the main strengths and weaknesses of the project and how it may contribute to the existing literature on this subject.

The results shown in the following sub-sections correspond to the cycles that were gradually refined in the period June 2005–June 2015 (10 years) under the (UNE71502, ISO17799, ISO27001:2005, ISO27001:2007, ISO27001:2013) standards. The scientific community has been provided with various contributions as regards partial results concerning the improvements made throughout the period of research.

5.1. Applying the Action-Research Method during the ISMS Development Phase

A description of how the cycles evolved, from the installation of the classic 'Security Management Plan' model to that of the current model in which the framework of MARISMA is applied, is shown as follows.

- *Cycle I1°*: Installing an ISMS using a classic process.
    - *Objective:* To install an ISMS in the SME.
    - *Characteristics:* An ISMS was installed and the whole process was developed to the customer's specifications. The following were carried out: a checklist by means of controls, a maximum level risk analysis and libraries of regulations and procedures, were carried out from scratch and were totally adapted. The greatest possible number of managers was involved in the development processes.
    - *Principal problems detected:* (i) It was impossible to organise work-related meetings without first reaching an agreement with all the managers involved; (ii) It was impossible to carry out a risk analysis owing to its detail and complexity; (iii) The users are against working with procedures on paper owing the huge amount of time needed to learn to do so; (iv) Difficulty involved in maintaining system updated and establishing corrective plans.
    - *Result:* The customer's general dissatisfaction with the result. The result obtained is complex and costly to maintain and is not aligned with the company's management. The customer does not believe that it is possible to attain an acceptable ROI.
    - *Duration*: 48 Weeks.

Since it was impossible to undertake the project because of its complexity for SMEs, a series of corrective cycles was initiated with the objective of resolving the various problems detected.

- *Cycle I2°*: Resolving aspects related to the risk analysis.
    - *Objective:* To simplify the risk analysis.
    - *Characteristics:* We sought to simplify the carrying out of the risk analysis by: (i) Selecting course-grained activities, i.e., activities that were as general as possible as opposed to being detailed; (ii) Simplifying the risk analysis.
    - *Principal problems detected:* The managers of the departments were more than ready to collaborate when asked to use few words to define between 2 and 5 groups of assets that

were of value to their departments. The problem of calculating and reviewing the risks was simplified to those risks related to the assets.
  - *Solution:* The simplification of the assets of which the information system is composed.
  - *Result:* The managers of the departments were more than ready to collaborate when asked to use few words to define between two and five groups of assets that were of value to their departments, rather than having to fill in a complex form in order to select assets and evaluations. This signified that the meeting and the asset selection processes were speeded up. Time was saved as regards calculating the risks and the risk reports, and the adaptations that have to be made when changing the value of assets.
  - *Associated with*: Activity A1.3 (T1.3.1–T1.3.4) and A2.4 (T2.3.1).
  - *Duration*: 44 Weeks.

- *Cycle I3°*: Resolution of aspects related to evaluating the level of security.
  - *Objective*: To simplify and increase the precision of the mechanism used to evaluate the level of security.
  - *Characteristics:* We sought to simplify and increase the precision of the activity that allows the company's current level of security to be determined.
  - *Principal problems detected:* When an auditor carries out an audit regarding the level to which the security controls are fulfilled, the results obtained tend to vary considerably when compared with those obtained by other auditors, thus making the evaluation of these controls very imprecise.
  - *Solution:* The establishment of a verification list at sub-control rather than control level.
  - *Result:* The controls were divided into more detailed questionnaires, thus reducing the margin of variation among the different auditors. Since these questionnaires are more focused, those responsible for security have less margin of error in the response and the level of evaluation can be carried out much more rapidly and efficiently.
  - *Associated with:* Activity A1.2 (T1.2.2).
  - *Duration*: 42 Weeks.

- *Cycle I4°*: Resolving aspects related to the risk analysis elements.
  - *Objective:* To automate the risk analysis processes and to reduce time.
  - *Characteristics*: We sought to simplify the performance of the risk analysis by predefining already existing relationships among its different elements.
  - *Principal problems detected*: The cost of determining the risk analysis elements (types of assets, vulnerabilities, threats, and risk criteria) involved for each company is high, but in different companies with similar characteristics (e.g., the same industrial sector) more than 90% of these relationships tend to coincide.
  - *Solution*: The creation of association matrices among each of the elements involved in the risk analysis. These matrices will be filled on the basis of the knowledge acquired during each of the installations and will associate two parts that are fundamental for the risk analysis: [Assets]–[Types of Assets, Vulnerabilities, Threats and Risk Criteria].
  - *Result:* Huge savings as regards the consultation task needed to establish the relationships among the risk analysis elements for each of the company's information system assets.
  - *Associated with:* Activity A1.3 (T1.3.5, T1.3.6, T1.3.8).
  - *Duration*: 39 Weeks.

- *Cycle I5°*: Resolving aspects related to the regulation and procedure libraries.
  - *Objective:* To increase the generation of procedures and regulations.

- *Characteristics:* We sought to simplify the creation of the procedures and regulations that form part of the ISMS by predefining the relationships among the different elements of the ISMS.
- *Principal problems detected*: The cost of creating made-to-measure procedures and regulations for each installation is huge and a detailed analysis of each process is required, in addition to involving a large number of technical personnel and company staff.
- *Solution:* The creation of association matrices among each of the elements involved in the regulations and procedures. These matrices will be filled on the basis of the knowledge acquired during each of the installations and will be associated with three parts that are fundamental for the generation of the ISMS: [Regulations]–[Procedures]–[Elements of the Procedures: (Phases, Technical Instructions, Registers, Templates, Routes and Profiles)].
- *Result:* Huge savings as regards the consultation tasks needed to define the map of the company's regulations and procedures.
- *Associated with:* Activity A1.4 (T1.4.1–T1.4.6).
- *Duration*: 31 Weeks.

- *Cycle I6°*: Resolving aspect related to regulation and procedure libraries.
  - *Objective*: To reduce costs as regards the generation and maintenance of procedures and regulations.
  - *Characteristics*: We sought to simplify the maintenance of the procedures and regulations that form part of the ISMS by establishing their relationships with the other ISMS elements.
  - *Principal problems detected*: In order to determine whether a procedure is necessary in the ISMS, it must be associated with the controls selected for the company by means of a consultation task.
  - *Solution:* The creation of association matrices among the regulations and procedures and the controls. These matrices will be filled on the basis of the knowledge acquired during each of the installations and will associate two parts that are fundamental for the generation of the ISMS: [Regulations]–[Controls]–[Procedures].
  - *Result:* Huge savings as regards the consultation tasks required to establish the procedures needed for the company's ISMS.
  - *Associated with:* Activity A1.4 (T1.4.7–T1.4.10).
  - *Duration: 28 Weeks.*
- *Cycle I7°*: Resolving aspects related to the risk analysis elements.
  - *Objective*: To associate the risk analysis with the other elements in the ISMS.
  - *Characteristics*: We sought to directly link the risk analysis elements with the system controls in order to unify all the elements of the ISMS.
  - *Principal problems detected*: The results of the risk analysis are left isolated from the rest of the ISMS, signifying that a costly task must later be carried out in order to determine how to associate the risks with the controls.
  - *Solution*: The creation of association matrices among the risk analysis and the controls. These matrices will be filled on the basis of the knowledge acquired during each of the installations and will associate the vulnerabilities with their associated controls.
  - *Result*: Huge savings as regards the consultation task needed to establish all the relationships among the risk analysis elements and the system controls. This new matrix allows all the elements in the system to be associated with its controls, thus enabling the majority of the processes to be automated.
  - *Associated with:* Activity A1.3 (T1.3.7).
  - *Duration*: 26 Weeks.

- *Cycle I8°*: Introduction of the concept of Schema [49].
    - *Objective*: To generate a structure that will permit knowledge reuse to be maximised (Schema).
    - *Characteristics*: The structure denominated as Schema will be capable of containing all the lists of the elements involved in the creation of an ISMS and the relationships that exist among them.
    - *Principal problems detected*: Having defined a set of matrices, we sought to automate and maximise its output, in addition to exploring the possibility of cloning these matrices so as to be able to carry out tests. It was also necessary to be able to incorporate any new elements that might appear during the research in an organised manner and to be able to distinguish these matrices on the basis of a series of characteristics (e.g., business sectors).
    - *Solution*: The creation of a structure that is capable of containing all the elements involved in the ISMS generation and maintenance process, which will additionally be able to involve new elements in its structure in a simple manner and to allow an unlimited number of configurations.
    - *Result*: Huge savings as regards the consultation task and the organisation needed to create the ISMS, since all the knowledge acquired in different installations is stored in the 'schema' structure.
    - *Associated with*: the SMSG sub-process.
    - *Duration*: 18 Weeks.
- *Cycle I9°*: Introduction of the concept of Maturity Level.
    - *Objective*: To establish evaluation processes and partial certification.
    - *Characteristics*: The introduction of partial certification and the concept of Maturity Level as an evaluation mechanism.
    - *Principal problems detected*: Many customers still considered the process to be very complex, and control points were therefore immediately required in order to deal with the projects with the closest deadlines.
    - *Solution*: The introduction of the possibility of establishing a certification and partial evaluation process by means of maturity levels. Tests were carried out with one level (cancel this concept), three levels, and five levels during the research. The results showed that SMEs tend to be more comfortable with a three-level system, although the process is carried out in such a way that variations are possible.
    - *Result*: Although involving a new management element implied an increase in costs, we consider that this cost is mitigated in the medium term by the improvements that it provides. The principal advantage is that it helps ensure that the installation and maintenance process will have a higher percentage of success.
    - *Associated with:* Activity A1.1 (T1.1.3).
    - *Duration*: 20 Weeks.
- *Cycle I10°*: Broadening the concept of Maturity Level.
    - *Objective*: To determine the maximum maturity level for a company by establishing a set of 'maturity rules'.
    - *Characteristics*: Determining the maximum maturity level that the company must attain on the basis of its current business structure.
    - *Principal problems detected*: Many customers attempt to comply with controls that exceed their current business capacity and overdimension the security management systems, which leads to an increase in risks in the medium term.

- *Solution*: The selection of a series of business characteristics that allows the determination of maximum maturity levels that it would be advisable for the company to attain, bearing in mind its current properties, with the objective of avoiding overdimensioning or assigning resources to controls of less priority. This was done by carrying out a study of the companies' characteristics and determining certain factors that influence their capabilities, and then establishing a simple algorithm that determines the most desirable level of security management at a particular moment.
- *Result:* Although involving a new management element implied an increase in costs, we consider that this cost is mitigated in the medium term by the improvements that it provides. The principal advantage is that it helps ensure that the installation and maintenance process will have a higher percentage of success.
- *Associated with:* Activity A1.2 (T1.2.1).
- *Duration*: 21 Weeks.

- *Cycle I11°*: Broadening the concept of Maturity Level.

  - *Objective*: To introduce the concept of Maturity Level into the Schema structure.
  - *Characteristics*: To introduce the concept of Maturity Level into the Schema structure in order to propagate its properties and advantages to the other elements in the schema.
  - *Principal problems detected*: The concept of Maturity Level contributes new characteristics to the ISMS, but a costly management task is required to apply it to the different objects.
  - *Solution*: The association of the levels of the sub-controls in the schema, such that they are propagated to all the elements in the ISMS, thus allowing the customer to know the maturity level of the security management at all times, and what must be done to attain the following level.
  - *Result*: A reduction in the costs associated with the introduction of the 'maturity level' element.
  - *Associated with:* Activity A1.2 (T1.2.2).
  - *Duration*: 17 Weeks.

- *Cycle I12°*: Establishing the concept of Maturity Level.

  - *Objective*: To introduce the concept of Current Maturity Level *(the level that company currently has, based on the formulas proposed in the methodology)* and the Desirable Maturity Level *(the level that the company should attain bearing in mind its current safety culture)* into the system installation and maintenance process.
  - *Characteristics*: The ability to determine the Current Maturity Level and the Desirable Maturity Level of the company's security management during the installation process, along with the overdimensioning of the security controls.
  - *Principal problems detected*: The customer wishes to have a simple means to know the current situation, the point that must be reached, and the recovery of resources in order to reach that point with guarantees.
  - *Solution*: The information needed to apply the algorithm that determines the company's current situation was obtained by: choosing the most appropriate schema for that company and using questionnaires in order to determine the current security level and the desirable security level.
  - *Result*: Although no savings were made as regards costs, the customer's knowledge and confidence in the process increased.
  - *Associated with:* Activity A2.2 (T2.2.1–T2.2.3).
  - *Duration*: 17 Weeks.

- *Cycle I13°*: Automating the risk analysis.
    - *Objective*: To automate the generation of the risk analysis in order to optimise the costs of this process.
    - *Characteristics*: The creation of algorithms that employ all the information obtained to generate a basic low-cost risk analysis.
    - *Principal problems detected*: The customer wished to be involved in the risk analysis process as little as possible, and wished above all else to minimise costs.
    - *Solution*: The information needed to apply an algorithm that would generate (i) a matrix of all the risks to which the assets were subjected and (ii) a simplified improvement plan to present to the customer, thus enabling him to understand how and why the improvement had been made, was obtained by choosing (i) the most appropriate schema for the company and (ii) a basic set of course-grained assets.
    - *Result*: Savings were made as regards costs, and a complete risk analysis that would be easy to maintain and regenerate was obtained.
    - *Associated with:* Activity A2.3 (T2.3.2).
    - *Duration*: 15 Weeks.
- *Cycle I14°*: Automating the elements of the ISMS.
    - *Objective*: To automate the selection and generation of the elements of the ISMS in order to optimise the costs of this process.
    - *Characteristics*: The creation of algorithms that utilise all the information obtained to select the most appropriate elements for the company's ISMS.
    - *Principal problems detected*: The process used to select the elements of which the ISMS should be composed required a consultant to carry out an analysis of all the information obtained until that time, which was a costly and complex process.
    - *Solution*: The information needed to apply an algorithm that automatically selects and installs the elements of which the ISMS is formed was obtained by choosing the most appropriate schema for the company and by using information obtained from the customer.
    - *Result*: Savings were made as regards costs, and an ISMS that was simple to maintain and regenerate was installed.
    - *Associated with:* Activity A2.4 (T2.4.1).
    - *Duration*: 12 Weeks.

A summary of how the different activities of which the SMScG and SMSyG processes are composed were introduced into the various cycles of the action-research method is provided in Figure 3.

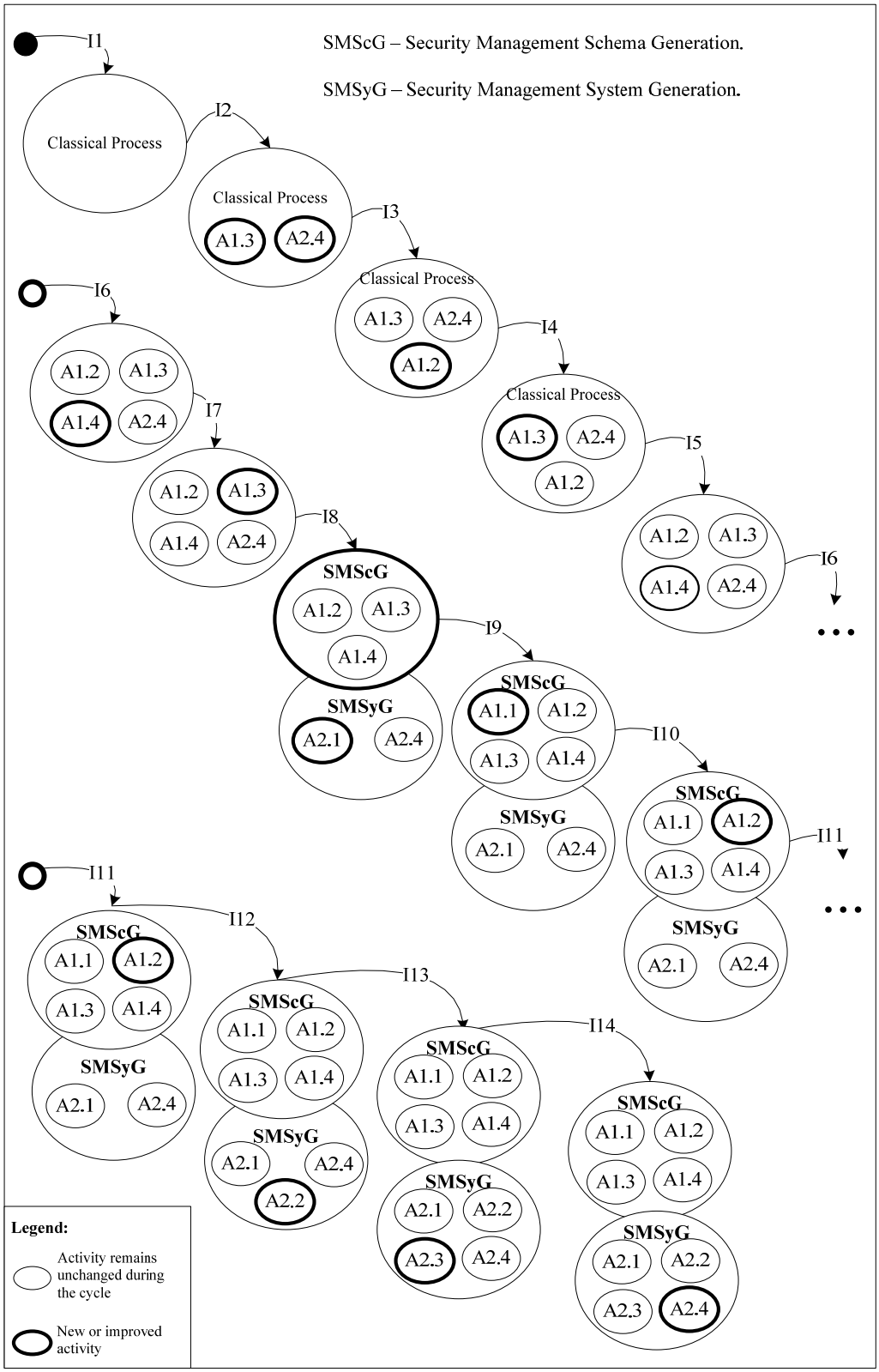

Figure 3. The use of AR to obtain the SMScG and SMSyG processes.

5.2. Conclusions Reached after Applying the Action-Research Method during the ISMS Development Phase

Figure 4 shows how the characteristics that allowed the ISMS generation and installation process to be reduced and improved were detected thanks to the application of the action-research method.

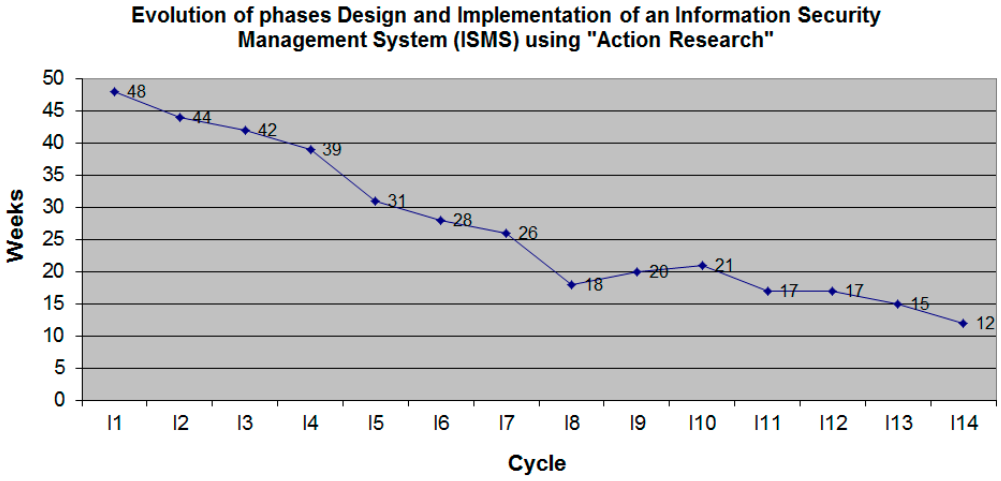

Figure 4. Evolution of the design and installation phases of an ISMS using AR.

We can also see that it was not always possible to decrease the amount of time required. There were some cycles, such as 19, during which it was necessary to increase the time needed for the system from 18 to 20 weeks in order to introduce concepts such as 'Maturity Level'. Despite making the system more costly in terms of time, these concepts were obviously necessary to maintain the quality of the system and were required by the companies involved. It is thus possible to conclude that the improvements made by using the Action-Research method do not always imply savings as regards time and resources.

It could be considered that the cost of the installation process is now suitable for SMEs, in addition to fulfilling all the characteristics that are required for the ISMS to be valid as regards both the principal standards and from the viewpoint of SMEs.

Having established the ISMS installation and generation phase, we shall now focus on optimising the maintenance processes.

As mentioned previously, these processes were evaluated in SMEs because these companies are more dependent on low-cost systems, and if the processes are valid for them, they will also be valid for large companies.

Table 1 shows an analysis of the estimated installation costs of the system in each of the cycles. The costs have been estimated with regard to the cases studied (Spanish SMEs with 10–50 employees in the autonomous regions of Castilla-La Mancha and Madrid), and the costs per hour may vary in the case of other countries. These costs have been extrapolated as the average of the estimates presented by the SNT Company to the research customers during the 10 years that the research lasted, for each phase in the cycle.

Table 1. Comparison of time taken and costs as regards consultations and customers for each iteration.

Cycle	Weeks	Consultantation Effort Hours	Consultant Time Cost (€)	Customer Personnel Effort Hours	Customer Personnel Time Cost (€)	Total Consultation Cost (€)	Total Cost to Customer (€)	Total Cost of Project (€)
I1	48	960	50	2880	20	48,000	57,600	105,600
I2	44	704	50	2464	20	35,200	49,280	84,480
I3	42	622	50	2184	20	31,080	43,680	74,760
I4	39	577	50	1794	20	28,860	35,880	64,740
I5	31	446	50	1364	20	22,320	27,280	49,600
I6	28	403	50	1176	20	20,160	23,520	43,680
I7	26	364	50	1144	20	18,200	22,880	41,080
I8	18	230	50	684	20	11,520	13,680	25,200
I9	20	272	50	840	20	13,600	16,800	30,400
I10	21	277	50	756	20	13,860	15,120	28,980
I11	17	218	50	612	20	10,880	12,240	23,120
I12	17	211	50	544	20	10,540	10,880	21,420
I13	15	180	50	450	20	9000	9000	18,000

It will be noted that the costs significantly decrease. The consultation projects carried out with the 'Security Management Plans' initially had consultation costs in the range of €40,000–50,000, and many companies confronted these by reducing the cost in time and by means of state subsidies in the form of 'Advancement Plans'. Thanks to the application of the Action-Research method, it was possible to attain a model in which both the consultation costs (approximately €9000) and those of the company (approximately €9000) were more reasonable. We nevertheless continue working to reduce these costs since, despite being valid for SMEs, they are not valid for MicroSMEs (less than 10 employees).

Table 2 shows how the consultation times are spread out during the installation of an ISMS when following the MARISMA methodology and how the tool is used to support that methodology in the current model.

Table 2. Description of cost in consultation hours for the MARISMA installation model in interaction 113.

Description of Activity (Mod-I13)	Hours
Pre-audit	16
Identification of assets	8
Risk Analysis and Management	24
Security Culture Course	8
Training regulation domains (14)	14
Consultation domains for the regulation.	49
Literal Training in the regulation	4
Literal consultation as regards the regulation.	25
Review and validation of documentation.	16
Internal audit	16

5.3. Applying the Action Research Method during the ISMS Maintenance Phase

Let us consider that it is possible to begin applying the action research method to the ISMS maintenance process:

- *Cycle M1°*: Initial process.
    - *Objective*: The users begin utilising the security management system.
    - *Characteristics*: (i) The procedures generated by the system are used on paper; (ii) There is no support tool; (iii) The level of security management is known every 2–3 years when a periodical audit is carried out.
    - *Principal problems detected*: (i) the users consider that it is very complicated to know the functioning of the procedures; (ii) the person responsible for security is overwhelmed by the cost of maintaining the system; (iii) not knowing which part of the system needs more resources leads the system to undergo progressive degradation.
    - *Solution*: Generalised changes as regards the way work is carried out.
    - *Result*: The current way of working leads to a medium-term failure rate in over 80% of the cases in which the system has been installed.
- *Cycle M2°*: Improvements oriented towards controlling the security level.
    - *Objective*: To discover the security level of the controls at all times.
    - *Characteristics*: The person responsible for security must, at all times, know which controls are degrading, with the objective of being able to balance the resources that are available.
    - *Principal problems detected*: Not knowing the level of security management so as to be able to control it in the short term signifies that it is not possible to take the measures that are necessary to prevent the system from functioning incorrectly.
    - *Solution*: The introduction of the concept of the scorecard.

- *Result*: The introduction of the concept of the scorecard led to a reduction in the failure rate of between 75% and 80%.
- *Associated with:* Activity A3.3.

- *Cycle M3°*: Improvements oriented towards controlling the security level.
  - *Objective*: The use of a tool and metrics to automate the maintenance of the security scorecard.
  - *Characteristics*: The person responsible for security must, at all times, know which controls are degrading with the objective of being able to balance the resources that are available, but it must not take much time to acquire this knowledge.
  - *Principal problems detected*: it is necessary to introduce the concept of the scorecard, but as this cannot depend on the continual audits carried out by the person responsible for security we must rather incorporate automation processes.
  - *Solution*: The introduction of a tool with metrics that will enable the security scorecard maintenance process to be automated.
  - *Result*: The introduction of the tool and the metrics led to a reduction in the failure rate of between 60% and 70%.
  - *Associated with:* Activity A3.3 (T3.3.1–T3.3.7).
- *Cycle M4°*: Improvements oriented towards procedure management.
  - *Objective*: To automate the use of the procedures by means of a tool.
  - *Characteristics*: The person responsible for security and the users must, at all times, know the functioning of all the procedures, although the majority of those procedures do not directly affect them.
  - *Principal problems detected*: The complexity of having to know all the procedures and comply with them manually leads to a large number of non-compliances and errors in the system, in addition to the users being generally against this means of working.
  - *Solution*: Extending the tool to contain the system procedures such that the users only have to interact with the part that directly affects them, thus signifying that they now only need to know the name and objective of the procedure.
  - *Result*: The automation of the procedures led to a reduction in the failure rate of between 30% and 40%, and greatly simplified work with the system.
  - *Associated with:* Activity A3.2 (T3.2.1–T3.2.2).
- *Cycle M5°*: Introducing the concept of the safety culture [50].
  - *Objective*: To introduce the system users to the concept of the safety culture.
  - *Characteristics*: The users tend to violate the regulations because they do not know them.
  - *Principal problems detected*: It was detected that the majority of the errors and failures in the system were the result of mistakes and a lack of knowledge of the regulations related to the system.
  - *Solution*: The users must be obliged to attain at least a minimum knowledge of the system in order to work with it, and should therefore be obliged to obtain a simple safety culture certificate that will guarantee this minimum knowledge.
  - *Result*: The introduction of the concept of the safety culture led to a reduction in the failure rate of between 20% and 30%, which is considered adequate as regards installing the ISMS with guarantees.
  - *Associated with:* Activity A3.1 (T3.1.1).

A summary of how the various activities of which the SMSyM process is composed were introduced into the different cycles of the action research method is provided in Figure 5.

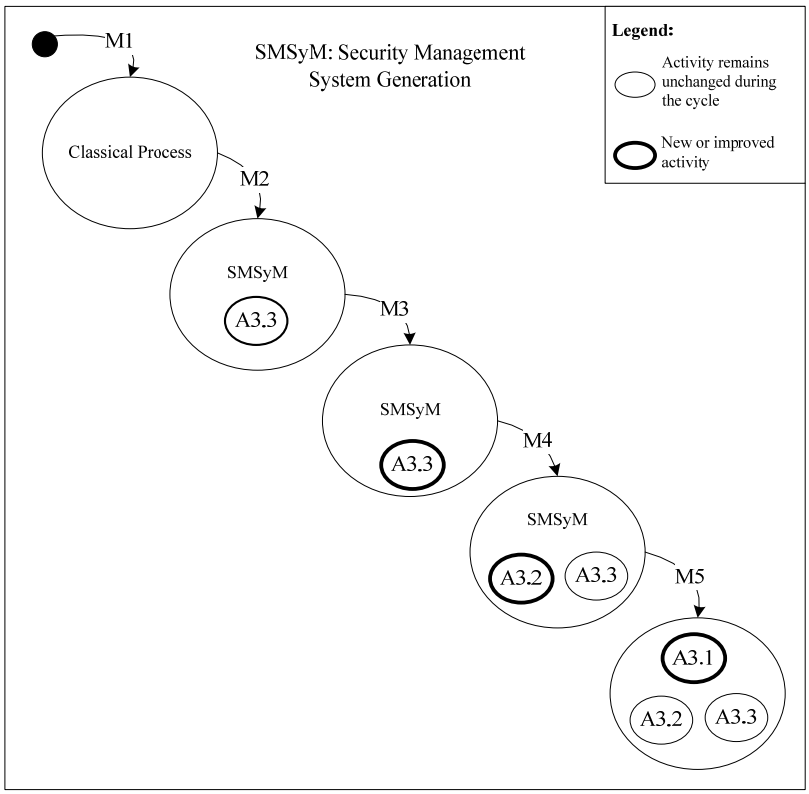

Figure 5. The use of AR to obtain the SMSyM processes.

5.4. Conclusions Reached after Applying the Action Research Method during the ISMS Maintenance Phase

Figure 6 shows how the characteristics that have allowed the ISMS maintenance process to be reduced and improved were detected thanks to the application of the action-research method.

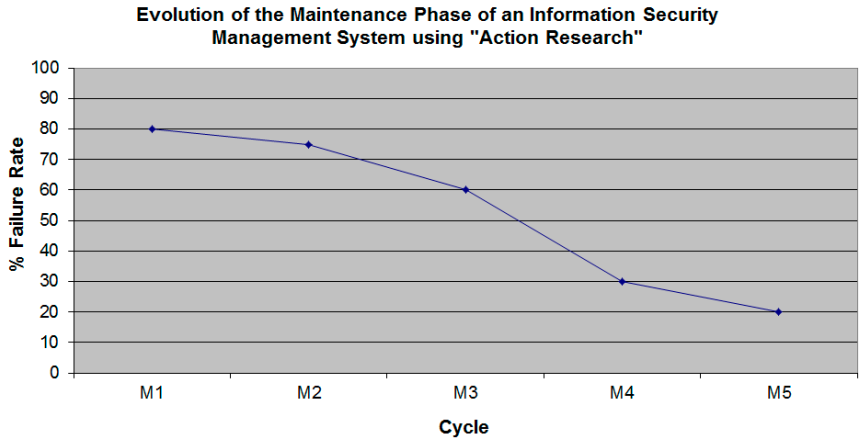

Figure 6. Evolution of the ISMS maintenance phases using AR.

Unlike that which occurred in the installation phase, none of the cycles in the maintenance phase supposed an increase in time. This was owing to the fact that the classic ISMS maintenance systems had been optimised to a very small extent and it was therefore possible to make great improvements to them during the application of the scientific method.

With the new application of the Action Research method to MARISMA it is becoming more difficult to attain considerable reductions in time, and the maintenance time of various cycles is rising rather than falling.

Table 3 therefore shows how the companies' internal costs associated with system maintenance have gradually been reduced from €3000/month to the current cost of €900/month. The majority of this cost can be attributed to the Person Responsible for Security. The table also makes it clear that the failure rate is related to the effort that the companies must make to invest in resources, which shows the importance of creating a low-cost model whilst always maintaining quality.

Table 3. Description of the costs in resources for the monthly maintenance of the company's ISMS.

Cycle	Internal Effort Hours/Month	Failure Rate	Customer Personnel Time Cost (€)	Total Cost to Customer (€)
M1	150	80	20	3000
M2	135	75	20	2700
M3	105	60	20	2100
M4	68	30	20	1350
M5	45	20	20	900

It is therefore possible to conclude that the AR method has allowed us to reduce the time and costs associated with installing an ISMS by 75%, while the initial failure rate of the system has been reduced by 70%, with some savings in the time the system users need to dedicate to security management tasks of 80%.

5.5. Strengths and Weaknesses of the Research

This sub-section shows the principal strengths and weaknesses of the research carried out.

- Strengths: We consider that the principal strength of this research has been its practical application in real cases, which has allowed us to carry out a genuine technological transfer of a problem that exists in the company, which has been resolved by applying a scientific method such as Action-Research. We can also conclude that the utility of the Action-Research method has been demonstrated within the field of Information Security Management Systems.
- Weaknesses: various events occurred during the research (a 10-year cycle) that obliged us to modify/adapt the research. Of these we should highlight the economic crisis of 2007, which led two companies to discontinue the use of their ISMS for financial motives, and these had to be replaced with two other similar companies. We can conclude that the principal weakness as regards applying the Action Research method to ISMSs is its slowness, since it is necessary to carry out cycles of various years in order to reach relevant conclusions.
- Contribution to existing literature: During the period of research we have shared the results obtained with the scientific community. This amounts to almost 100 contributions (two books, three book chapters, more than 20 papers in journals, more than 40 publications at congresses, and more than 25 professional presentations). These have served to enrich the methodology upon obtaining the validation of the lessons learnt after applying the Action-Research method and providing the customers with improvements. The publications were oriented towards not only the scientific but also the professional community. This research therefore supposes an important contribution towards the existing literature on Information Security Management Systems.

6. Conclusions

In this paper we have presented how the application of the action research (AR) method allowed us to make improvements to one methodology and to obtain another new methodology for the more efficient installation of Security Management Systems in companies.

The analysis of the AR cycles has enabled us to show how the cost and effort needed to install an ISMS have been reduced to a level that companies consider acceptable and how knowledge reuse allowed us to reduce resources by almost 75%.

The characteristics provided by the methodology and its orientation towards SMEs have been very well received, and its application is proving to be very positive. This is because it allows this type of company to use information security management systems at a cost that is considered acceptable in terms of both the money invested and human resources, which has, until now, been possible only for large businesses. This research method has also allowed us to make improvements to the methodology, obtain short-term results, and reduce the costs that the use of other methodologies implies, thus satisfying the company to a greater extent.

It is currently possible to consider that the version obtained fulfils the necessary requirements for it to be valid for both SMEs and large companies, but we shall continue to apply the AR method with the objective of identifying ways in which the methodology could be improved, and although these improvements will not have the same impact as the first cycles, they will suppose appreciable changes without implying an increase in costs.

In summary, the results obtained after applying the method were:

- A suitable method with which to manage security and its level of maturity in SMEs' information systems.
- A security maturity and management model based on the methodology developed and denominated as the base schema, which is appropriate for the resources of SMEs. The result was accepted by the critical reference group.
- Benefits for the participants: scientific benefits for the researcher and practical benefits for the beneficiaries.
- The knowledge obtained can be applied immediately.

The research has been developed in a typically cyclical and iterative process, combining theory and practice.

All future improvements to the methodology and the model are oriented towards improving their precision whilst always respecting the principle of costs of resources, i.e., we seek to improve the model without incurring costs associated with generating and maintaining the ISMS.

In conclusion, we can state that we have demonstrated the enormous value provided by qualitative research methods when improving processes such as security management as regards both obtaining a valid methodology and applying a continuous improvement process to it.

The research is currently continuing with a refinement process and continuous improvements to the methodology. It is being validated in the original companies in Spain, and also through its incorporation into new companies in other countries such as Colombia, Ecuador, and Peru.

Acknowledgments: This research has been partially co-funded by the ERABAC (1315ITA227) and ESACC (1315ITA225) projects, financed by the "D.G. de Empresas, Competitividad e Internacionalización de la Consejería de Economía, Empresas y Empleo de la JCCM"; the SIGMA-CC (TIN2012-36904) and GEODAS (TIN2012-37493-C03-01) projects, financed by the "Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER" (España); the SERENIDAD (PEII14-2014-045-P) project, financed by the "Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla-la Mancha and the el Fondo Europeo de Desarrollo Regional FEDER" (España), as part of the "Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad-Código: ESPE-2015-PIC-019" Project, financed by the ESPE and CEDIA (Ecuador); and the PROMETEO Project, financed by the Ecuadorean government's Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT).

Author Contributions: Luis Enrique Sánchez and Antonio Santos-Olmo have contributed to the design, development, and validation of the research in the private sector. David G. Rosado, Eduardo Fernández-Medina, and Mario Piattini have contributed to the design, development, and validation of research from the perspective of a university.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Von Solms, R. Information Security Management: Processes and Metrics. Ph.D. Thesis, Degree-Granting University, Johannesburg, South Africa, 2014.
2. Santos-Olmo, A.; Sánchez, L.E.; Rosado, D.G.; Fernández-Medina, E.; Piattini, M. Aplicación del método de Investigación-Acción para desarrollar una Metodología Ágil de Gestión de Seguridad de la Información. In Proceedings of the VIII Congreso Iberoamericano de Seguridad Informática (CIBSI15), Quito, Ecuador, 10–12 November 2015; pp. 14–27. (In Spanish).
3. Candiwan, C. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. In Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), Kuala Lumpur, Malaysia, 17–19 November 2014; pp. 50–58.
4. Whitman, M.; Mattord, H. *Principles of Information Security*; Cengage Learning: Boston, MA, USA, 2012.
5. Lampson, B.W. Computer Security in the Real World. *IEEE Comput. Soc.* **2004**, *37*, 37–46. [CrossRef]
6. Whitman, M.; Mattord, H. *Management of Information Security*; Cengage Learning: Boston, MA, USA, 2013.
7. Lampson, B. Protection. *ACM Oper. Syst. Rev.* **1974**, *8*, 18–24. [CrossRef]
8. Saltzer, J.H. Protection and the Control of Information Sharing in Multics. *Commun. ACM* **1974**, *17*, 388–402. [CrossRef]
9. Denning, E.D. A lattice model of secure information flow. *Commun. ACM* **1976**, *19*, 236–243. [CrossRef]
10. Ellison, C. SPKI Certificate Theory. Available online: http://www.ietf.org/rfc/rfc2692.txt (accessed on 11 July 2016).
11. Vivas, T.; Zambrano, A.; Huerta, M. Mechanisms of security based on digital certificates applied in a telemedicine network. In *Engineering in Medicine and Biology Society, 2008. EMBS 2008*, Proceedings of the 30th Annual International Conference of the IEEE, Vancouver, BC, Canada, 20–24 August 2008.
12. Sandhu, R. Role-Based Access Control Models. *IEEE Comput.* **1996**, *29*, 38–47. [CrossRef]
13. Eloff, J.; Eloff, M. Information Security Management—A New Paradigm. In Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology (SAICSIT '03), Fourways, South Africa, 17–19 September 2003; pp. 130–136.
14. Disterer, G. Iso/iec 27000, 27001 and 27002 for information security management. *J. Inf. Secur.* **2013**, *4*, 92–100. [CrossRef]
15. Beckers, K.; Faßbender, S.; Heisel, M.; Küster, J.C.; Schmidt, H. Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches. In *Engineering Secure Software and Systems*; Barthe, G., Livshits, B., Scandariato, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 14–21.
16. Dhillon, G. *Managing Information System Security*; M.P. Ltd., Ed.; Palgrave Macmillan: London, UK, 1997.
17. Kemmerer, R.A. Cybersecurity. In Proceedings of the 25th International Conference on Software Engineering, Portland, OR, USA, 10 May 2003.
18. Baskerville, R. The development duality of information systems security. *J. Manage. Syst.* **1992**, *4*, 1–12.
19. McDermott, J.; Fox, C. Using Abuse Case Models for Security Requirements Analysis. In Proceedings of the 15th Annual Computer Security Applications Conference, Phoenix, AZ, USA, 6–10 December 1999.
20. Anderson, C. *The Long Tail: How Endless Choice Is Creating Unlimited Demand*; Random House Business Books: London, UK, 2006.
21. Householder, A.; Houle, K.; Dougherty, C. Computer attack trends challenge Internet security. *IEEE Comput.* **2002**, *35*, 5–7. [CrossRef]
22. James, H.L. Managing information systems security: A soft approach. In Proceedings of the Information Systems Conference of New Zealand, Palmerston North, New Zealand, 30–31 October 1996.
23. Papazafeiropoulou, A.; Pouloudi, A. The Government's Role in Improving Electronic Commerce Adoption. In Proceedings of the European Conference on Information Systems 2000 Conference, Wienna, Austria, 3–5 July 2000.
24. Dimopoulos, V.; Furnell, S.; Jennex, M.; Kritharas, I. Approaches to IT Security in Small and Medium Enterprises. In Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future, Perth, Australia, 26 November 2004; pp. 73–82.
25. Gupta, A.; Hammond, R. Information systems security issues and decisions for small businesses. *Inf. Manage. Comput. Secur.* **2005**, *13*, 297–310. [CrossRef]

26. Helokunnas, T.; Iivonen, L. Information Security Culture in Small and Medium Size Enterprises. In *e-Business Research Forum—eBRF 2003*; Tampere University of Technology: Tampere, Finland, 2003.
27. ISBS. *Information Security Breaches Survey 2006*; Department of Trade and Industry: London, UK, 2006.
28. Furnell, S.M.; Gennatou, M.; Dowland, P.S. Promoting Security Awareness and Training within Small Organisations. In Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia, 7 November 2000.
29. Johnson, D.W.; Koch, H. Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Maui, HI, USA, 4–7 January 2006.
30. O'Halloran, J. ICT business management for SMEs. *Comput. Wkly*. Available online: http://www.computerweekly.com/feature/ICT-business-management-for-SMEs (accessed on 4 June 2016).
31. Doherty, N.F.; Fulford, H. Aligning the Information Security Policy with the Strategic Information Systems Plan. *Comput. Secur.* **2006**, *25*, 55–63. [CrossRef]
32. Seaman, C.B. Qualitative Methods in Empirical Studies of Software Engineering. *IEEE Trans. Softw. Eng.* **1999**, *25*, 557–572. [CrossRef]
33. Avison, D.; Lau, F.; Myers, M.D.; Nielsen, P.A. Action research. *Commun. ACM* **1999**, *42*, 94–97. [CrossRef]
34. Genero, M.; Cruz-Lemus, J.A.; Piattini, M. *Métodos de Investigación en Ingeniería del Software*; Editorial RA-MA: Madrid, Spain, 2014; pp. 171–199.
35. Bugdol, M.; Jedynak, P. *Integration of Standardized Management Systems, In Integrated Management Systems*; Springer: Cham, Switzerland, 2015; pp. 129–160.
36. Bugdol, M.; Jedynak, P. *Integrated Management Systems*; Springer: Cham, Switzerland, 2015.
37. International Organization for Standardization. *ISO/IEC 27001:2013, Information Technology—Security Techniques Information Security Management Systemys—Requirements*; International Organization for Standardization: Geneva, Switzerland, 2013.
38. International Organization for Standardization. *ISO/IEC 27002:2013, the International Standard Code of Practice for Information Security Management (en desarrollo)*; International Organization for Standardization: Geneva, Switzerland, 2013.
39. COBIT 5. *Cobit Guidelines, Information Security Audit and Control Association*; ISACA: Rolling Meadows, IL, USA, 2012.
40. Batista, J.; Figueiredo, A. SPI in very small team: A case with CMM. *Softw. Process Improv. Pract.* **2000**, *5*, 243–250. [CrossRef]
41. Hareton, L.; Terence, Y. A Process Framework for Small Projects. *Softw. Process Improv. Pract.* **2001**, *6*, 67–83.
42. Tuffley, A.; Grove, B.; McNair, G. SPICE for Small Organisations. *Softw. Process Improv. Pract.* **2004**, *9*, 23–31. [CrossRef]
43. Villalon, J.A.C.M.; Agustin, G.C.; Gilabert, T.S.F.; Seco, A.D.A.; Sanchez, L.G.; Cota, M.P. Experiences in the Application of Software Process Improvement in SMES. *Softw. Qual. J.* **2004**, *10*, 261–273. [CrossRef]
44. Mekelburg, D. Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. *Softw. Qual. Prof.* **2005**, *7*, 4–13.
45. Sánchez, L.E.; Santos-Olmo, A.; Fernández-Medina, E.; Piattini, M. ISMS Building for SMEs through the Reuse of Knowledge. In *Small Medium Enterprises: Concepts, Methodologies, Tools, Applications*; IGI Global: Hershey, PA, USA, 2013; p. 394.
46. Sánchez, L.E.; Parra, A.S.O.; Rosado, D.G.; Piattini, M. Managing Security and its Maturity in Small and Medium-sized Enterprises. *J. Univers. Comput. Sci.* **2009**, *15*, 3038–3058.
47. Santos-Olmo, A.; Sánchez, L.E.; Fernández-Medina, E.; Piattini, M. Desirable Characteristics for an ISMS Oriented to SMEs. In Proceedings of 8th International Workshop on Security in Information Systems (ICEIS 2011), Beijing, China, 8–11 June 2011; pp. 151–158.
48. Santos-Olmo, A.; Sánchez, L.E.; Fernández-Medina, E.; Piattini, M. A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs. In Proceedings of the 9th International Workshop on Security in Information Systems (WOSIS12), Wroclaw, Poland, 28 June 2012; pp. 117–124.

49. Sánchez, L.E.; Santos-Olmo, A.; Fernández-Medina, E.; Piattini, M. Building ISMS Through Knowledge Reuse. In Proceedings of the 7th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS'10), Bilbao, Spain, 30–31 August 2010.
50. Sánchez, L.E.; Santos-Olmo, A.; Fernández-Medina, E.; Piattini, M. *Security Culture in Small and Medium-Size Enterprise, In ENTERprise Information Systems*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 315–324.