Assessing a simplified Information Security approach

Feedback from RA/RM Pilot

February | 09

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on Risk Management for SMEs, please use the following details:

Daniele Catteddu, Junior Expert Risk Management
Dr. Louis Marinos, Senior Expert Risk Management
e-mail: RiskMngt@enisa.europa.eu
Internet: http://www.enisa.europa.eu/rmra

Table of Contents

About ENISA 2

Contact details: 2

EXECUTIVE SUMMARY 6

1. INTRODUCTION 7

2. STRUCTURE OF THE DOCUMENT 7

3. OBJECTIVE OF THE PROJECT 8

4. ORGANIZATION INVOLVED IN THE PROJECT 8

5. IDENTIFIED ISSUES 11

5.1 Outsourcing Options 11

5.2 Risk Profile Selection 13

5.2.1 Legal and Regulatory impact 13

5.2.2 Productivity impact 14

5.2.3 Financial stability impact 15

5.2.4 Reputation and loss of customer confidence 16

5.3 Critical Asset Identification 16

5.4 Control Cards Selection 19

5.5 Implementation and Management 21

5.5.1 Gap Analysis 21

5.5.2 Mitigation Plan 22

6. CONCLUDING CONSIDERATIONS 22

7. ROAD MAP FOR IMPROVEMENT 24

8. REFERENCES 25

1.A INTRODUCTION 27

2.A METHODOLOGY RELATED ISSUES 28

DECISION MAKERS AND OUTSOURCING 29

RISK PROFILE SELECTION 29

Statement of application 29

Modifications proposed 30

CRITICAL ASSET IDENTIFICATION 31

Statement of application 31

Modifications proposed 32

ORGANIZATIONAL CONTROL CARD SELECTION 33

Statement of application 33

Modifications proposed 33

IMPLEMENTATION AND MANAGEMENT 34

FINAL CONSIDERATIONS 34

3.A FUTURE WORKS 35

1.B INTRODUCTION 38

BACKGROUND INFORMATION 38

SCOPE AND OBJECTIVES OF THE PILOTS 38

2.B SELECTION OF FIRMS AND DEPLOYMENT OF PILOTS 39

SELECTION OF FIRMS 39

APPROACH FOLLOWED IN THE DEPLOYMENT 39

VALIDATION OF THE PILOTS 40

3.B COMMENTS AND ISSUES IDENTIFIED 41

BASIC APPROACH 41

OUTSOURCING OPTIONS 41

RISK PROFILE SELECTION 42

Legal and Regulatory *42*
Productivity and financial stability *42*
Reputation and Loss of Customer Confidence *42*
Asset Selection *43*
Card Selection *43*
Card contents *44*
Gap analysis *44*
4.B GENERAL FINDINGS 44
1.C INTRODUCTION 50
BACKGROUND OF THE PILOT 50
OBJECTIVE OF THE PILOT 50
SELECTION OF THE SMES AND MICRO ENTERPRISES 51
PLANNING AND ORGANIZATION OF WORK 53
2.C METHODOLOGY DEPLOYMENT 59
3.C METHODOLOGY RELATED ISSUES. 61
OUTSOURCING OPTIONS 61
RISK PROFILE SELECTION 61
ASSET IDENTIFICATION 63
CONTROL CARDS SELECTION 64
IMPLEMENTATION AND MANAGEMENT/ GAP ANALYSIS 68
4.C GMS'S GENERAL COMMENTS AND OBSERVATIONS 69
5.C GENERAL FINDINGS 71
6.C FEEDBACK FROM COMPANIES 72
7.C REFERENCES 74

Executive Summary

ENISA's effort to create awareness in Small Medium Enterprises (SMEs) and Micro Enterprises (MEs) started in 2007. The objective was to stress the fundamental role of risk assessment and management in the protection of IT-infrastructure. This has been achieved with the ENISA deliverable "Information Package for SMEs" (see "ENISA Deliverable: Information Package for SMEs"). In this document, a simplified approach to risk assessment and some aspects of risk management are been described.

In 2008 ENISA started a set of pilots to validate and promote this approach, receive feedback from the involved enterprises and to identify possible adaptations to the approach depending on the size, sector and level of exposure of the participants.

ENISA launched a call for expression of interest in February 2008 to identify potential partners to be involved in a Risk Assessment/Risk Management (RA/RM) activity. In order to involve the biggest number of SMEs and MEs as possible in the pilot, the proposals of three multipliers organization were selected by ENISA.

The pilot had a threefold objective:
(1) Validate the content of the simplified approach,
(2) Evaluate the applicability of the proposed RA/RM approach and
(3) Collect feedback and proposal for changes.

After the finalization of the projects the following conclusions can be drawn:

- The ENISA simplified RA/RM approach received a generally high level of appreciation from the approx. 15 MEs and SMEs involved in the pilot.
- The ENISA simplified RA/RM approach led to an increased level of awareness on the fundamental role of Information Security Risk Assessment and Management. The pilots generated the impression, that the companies involved in the project were more motivated to improve their information security management approaches.
- It is unlikely that both SMEs and MEs could use the RA/RM simplified approach as such without an external support, at least for the first implementation.
- Some simplifications/automated steps might be required to better target the audience of very small and micro enterprises.
- The multipliers agreed on the need to introduce some customizations to the ENISA approach (e.g. sector-based and market-segment-based etc.).
- ENISA's strategy to involve multiplier organizations in the pilot was widely accepted by all participants. A further involvement of such partners in information security awareness raising process seems to be necessary.

Apart from serving as a road-map for future ENISA activities in the area of SMEs, this document can be used by interested individuals to better understand the requirements of SMEs, and possibly take identified requirements into account in their professional activities.

1. Introduction

In its efforts to promote Information Security ENISA has generated material that helps small and medium enterprises (SMEs) to understand and to apply Risk Assessment and Risk Management to secure their IT infrastructure. In this context, the report "ENISA Deliverable: Information Package for SMEs" was published as a part of the ENISA Work Programme 2006.

The "Information Package for SMEs" is the first ENISA's attempt to address the issue of Risk Assessment and to some extent Risk Management (also referred to in the rest of this document as *ENISA simplified RA/RM approach*). The approach taken is a one-size-fits-all solution created for non-expert users and for small organisations with relatively simple IT-components. One of the main drivers that have pushed ENISA towards a simplified Risk Assessment and Management approach was the idea that SMEs need simple, flexible, efficient and cost-effective security solutions.

The philosophy behind the generation of the simplified approach was to guide non-expert users in the complexity of risk assessment and risk management activities. In doing so, some complex security matters have been simplified to the minimum necessary in order to achieve an acceptable security level. This lead to a step-wise approach that reveals threat exposure from user by offering customized controls for a certain set of assets that are common to the IT environment of SMEs.

Given the role of ENISA to promote culture of security (mentioned in its regulation 460/2004 of the European Parliament and of the Council of 10 March 2004) a preparatory activity with the title "Building Information Confidence with Micro Enterprises" has been included in the Work Programme 2008. Within this activity a call for expression of interest was launched. The objective was to involve SMEs in the implementation of the "Information Package for SMEs", to generate awareness for SMEs and micro-enterprises and evaluate the ENISA approach.

Three multiplier organizations were selected for the Pilot, namely GMV Soluciones Globales Internet (Spain), IAAITC (UK) and University of Bologna (Italy). Each multiplier brought in some representative SMEs/micro-enterprises from their areas/sectors.

More than 10 pilots were performed to check the applicability of the simplified Risk Assessment and Management approach. The results of the pilots have been collected and consolidated by means of the present report. The particular reports submitted by the pilots [1]are also available and will be published as additional material to this report (see Annexes).

2. Structure of the document

The document is structured as follows:

[1] *The reports from the pilots are anonymised, that is, they do not reveal any confidential information from the risk assessments of the participating companies.*

Sections 3 and 4 describe the objectives of the pilot action and the organizations involved in the project.

Section 5 reports about the comments from each pilot, while ENISA's considerations on the received comments are included. All issues identified within the feedback from the pilots are categorized in phases according to the structure of the ENISA approach.

Section 6 highlights the final considerations.

Section 7 summarises by presenting a roadmap for possible improvement of the ENISA approach. Forthcoming developments of the ENISA simplified approach will be based on the points of this roadmap.

Finally, material from the pilots has been attached in form of annexes to better help understanding the findings from the pilots.

3. Objective of the project

The main objectives of the project were to:

- Assess the level of awareness on Risk Assessment and Management in SMEs of various types (i.e. size and sector) and try to raise awareness by introducing the ENISA simplified approach in these SMEs.
- Evaluate the applicability of the simplified Risk Assessment & Management approach for SMEs in "real word" situations and
- Get feedback from the pilots in order to improve the approach and increase the potential value for SMEs.

Regarding the entire process applied for the life-cycle of the simplified approach, ENISA has applied the Plan-Do-Check-Act model:

- PLAN: creation of a simplified Risk Assessment & Risk Management approach for SMEs (already performed in 2006-2007)
- DO: run pilots in different contexts inside EU (performed in 2007-2008)
- CHECK: get feedback from pilots and aggregate and analyze it (received in 2008)
- ACT: review and improve the simplified approach starting from the feedback (in 2009 and beyond)

It is expected that through repetitions of the above life-cycle a proper maturity of the simplified ENISA method will be achieved. Further steps in this direction are the activities planned for 2009 concerning the deployment of the simplified approach with the support of a multiplier organisation (see ENISA Work Program 2009:

4. Organization involved in the project

The selection process following the expression or interest led to the awarding of proposals form multiplier organizations; the rationale behind this choice was to guarantee the inclusion of multiple medium/small/micro enterprises in each pilot.

The following multiplier organisations have been awarded:

- **CESIA – University of Bologna (Italy)**

Business Sector: Public administration, Education

University of Bologna applied the RA/RM method in three categories of departments:

- ✓ Small Departments
- ✓ Medium Departments
- ✓ Large Departments

There were seven departments involved in the exercise. With the CESIA case, a federated model of quasi autonomous entities attached to an outsourcer has been covered. Given current trends in security, this model is being considered as an interesting one, especially in the area of small public authorities.

The report from the pilots at the University of Bologna can found in:

http://www.enisa.europa.eu/rmra/files/rm_pilot_italy.pdf

- **GMV Soluciones Globales Internet, S.A. (Spain)**

Business Sector: Outsourcer of information Security Services

Four companies have been involved by GMV in the exercise, ranging from micro businesses to medium enterprises with ca. 100 employees.

The companies were selected by GMV with the support of CEEI (Centros Europeos de Empresas e Innovacion de Castilla y Leon), a multiplier organisation supporting small businesses. The companies chosen for the pilot were:

- ✓ Machine Point
- ✓ Instituto Biomar
- ✓ Proxima
- ✓ Besel

GMV is one major Spanish consulting firm performing security assessments and risk management consultancy. The GMV case is the typical scenario where risk assessment and risk management practices are performed on behalf of customers (i.e. GMV acts as outsourcer of security practices). This scenario is one of the most common in risk management businesses for small enterprises.

The report from the Spanish pilots can be found in:

http://www.enisa.europa.eu/rmra/files/rm_pilot_spain.pdf

- **IAAITC (UK)**

Business Sector: Association, accounting

There were six firms brought in by IAAITC, ranging from micro businesses to professional practice with 150 employees.

The six businesses that participated in the implementation of the RA/RM approach were:

- ✓ Accountants (NDA)
- ✓ Training College (Journalists) (NDA)
- ✓ Scientific Membership Society (NDA)
- ✓ Event Management (NDA)
- ✓ Financial Services (NDA)
- ✓ Physiotherapy Services (NDA)

IAAITC is an association of accountants who also provide IT-consultancy to their customers. Given the trust relationship between small companies of any size and their accountants, with this pilot the concept of "train the trusted party" has been applied. In other words, a knowledge transfer took place to the point of service (i.e. the accountant company). Accountant firms have suggested their customers as participants to the pilot, while the accountant itself was part of the risk assessment team.

The report of IAAITC can be found in:

http://www.enisa.europa.eu/rmra/files/rm_pilot_uk.pdf

5. Identified issues

All the comments raised from the pilots are grouped according to the components of the simplified RA/RM approach.

The method is depicted in the Figure 1 below.

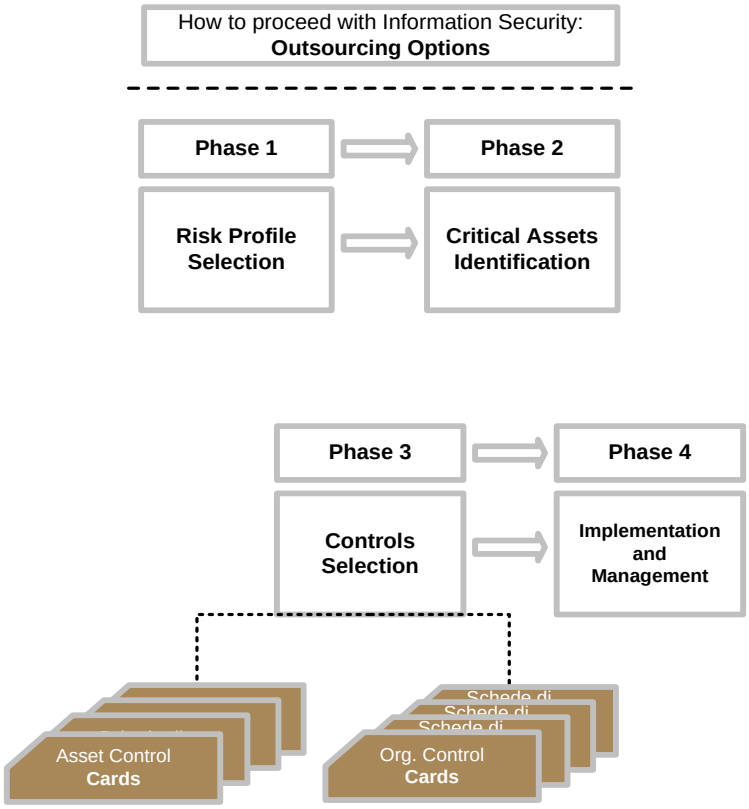


Figure 1: Overview of the phases of the ENISA simplified approach

The **Outsourcing Options** together with the four phases depicted in the figure above are used as titles for the sections of this chapter. For each comment received ENISA provided its own considerations.

5.1 Outsourcing Options

The Outsourcing Options are described in the Chapter 3 of the Information Package for SMEs. This is the first step in the risk assessment activity in which the make-or-buy decision is taken. This step is the precondition for all other four phases of simplified RA/RM approach.

Outsourcing Options	
CESIA	No relevant comments.
IAAITC	In the opinion of IAAITC, this phase could be simplified. It is also pointed out, that there are the following problems in the questions asked: • According to the report, if for example the assessment takes place for a micro business, asking whether they can make available two to five people for the assessment project is probably not an appropriate question, as this personnel availability does not exist at all. • Another problem they raised concerns the inappropriate use of the English language • They suggest a simpler breakdown, as follows: • Do you have the time available within your organisation to carry out this review? • Do you have the knowledge available in your organisation to carry out this review? • Do you want an external assessment of your Risk Management position? IAAITC believes that based on these questions a business should be able to decide whether they wish to carry out the review in-house, outsource all of the review to an external assessment body, or a combination of the two. Another possible option they have proposed is to award points to each question and introduce an element of weighting in the survey (i.e. On a scale of 1 to 10, rate your IT knowledge). The decision on whether to outsource can then be based on the overall score.
GMV	GMV, being a consulting services firm in the information security industry, participated as an outsourcer of the risk assessment for the companies involved in the pilot. There are two main arguments for this choice: 1. GMV had a hybrid approach to the Pilot. In fact they combined the RA/RM simplified approach from ENISA with a tool named **PILAR.** Pilar is based on the Magerit Risk Analysis Methodology that is being used widely in Spain. 2. None of the involved companies have had sufficient knowledge on Risk Analysis and Risk Management. In addition, they didn't have enough human resources to perform this task, even in the case that GMV could give them enough training to do so.

	GMV performed a Pre-Assessment, using a preliminary questionnaire to verify the *status quo* of the companies involved in the exercise. The preliminary questionnaire was a customization of the information package provided by ENISA.
ENISA	The suggestion from IAAITC can lead to consensus. The preparatory phase in which the make-or-buy decision is taken needs to be reviewed according to the suggestions and possibly simplified. In this effort, the techniques applied by GMV could be taken as an example for possible simplifications/re-adjustments.

5.2 Risk Profile Selection

In the Risk Profile Selection Phase (Phase 1) the risk profile of an organization is defined using a predefined set of qualitative criteria Used criteria refer to various areas of impact that a loss might cause. Legal Regulatory, Productivity and Financial impact is being accounted for. This phase is of fundamental importance, as it sets level of exposure of the assessed organisation. All other phases depend on phase 1.

5.2.1 Legal and Regulatory impact

Legal and Regulatory impact	
CESIA	No relevant comments.
IAAITC	The IAAITC comment is: "*(in the ENISA simplified approach)* the sensitivity of the data held focuses on third party data. However, many organisations hold information on their own organisation, products and services which would also represent a major business risk if accessed by unauthorised people. Examples include all forms of Intellectual Property (IP), such as product information for technology companies. The criteria for this profile could be based on questions to the business to identify what they consider to be the most valuable information held and then assigning an impact to loss or disclosure of that data by unauthorised users."
GMV	No relevant comments about the specific area of risk. GMV provided some general consideration for the Risk Profile Selection Phase. Firstly, it is worth mentioning that GMV turned the entire contents of this phase into a questionnaire. In addition to the above, GMV delivered the following generic comment for the entire ENISA simplified approach: is the following: "for determining the company profile, the ENISA approach does not take into account the three common requirements of security namely: Integrity, Confidentiality and Availability.

	GMV has also added that taking into account these three main security requirements, would be of interest during safeguards selection or within the recommendation of protection levels of the relevant assets.
ENISA	The comment from IAAITC is good starting point for a general improvement of the used terminology/examples. As a matter of fact IP is considered to be an asset that can have Legal and Regulatory impact. In fact, the business risk related to the loss of confidentiality of sensitive information (Intellectual Property, know-how, etc.) seems to have a clear relevance with the Financial Stability of the organisation (see category below). On the other hand, it would be eventually possible to extend the risk profile definition to include the need for compliance to sector-based regulations and/or good practices (i.e. PCI DSS), corporate governance regulations (for High risk profile) and contractual liability. With regard to the feedback from GMV, it is a valuable idea to have a questionnaire-like approach for this phase. This could help businesses to better position themselves in the appropriate area of risk exposure. One of the Spanish pilots (according to GMV report, the most proactive SME in the project) confirmed that the questionnaire-like approach was very helpful in their particular case. On the other hand, it is not the case that RA/RM simplified approach does not take into account the three common requirements of the security: Integrity, Confidentiality and Availability. As a matter of fact, in the Critical Asset Identification phase ENISA included an evaluation of security requirements (Integrity, Confidentiality and Availability) for the most important assets.

5.2.2 Productivity impact

Productivity impact	
CESIA	The University of Bologna replaced "Productivity" and "Financial Stability" with "Teaching", "Research" and "Patents". The change was made to better fit the needs of the University. Similar adaptations/additional examples might be necessary for other sectors (e.g. public administration, health, etc.).
IAAITC	IAAITC argued that dimensions like turnover and number of employees possibly allows scope for error. For instance, a number of the pilot businesses felt that this seemed to bias the survey to show small organizations as being low risk, whereas in many cases this would be not true. They report also a gap in the financial criteria listed.

	The other point that IAAITC raised is that any financial criteria need to take into account the business type (i.e. a small car dealership may have a very high turnover because it deals in high value goods, but an accountancy firm may have limited turnover because the only sales are service costs). Furthermore, they underlined that the person carrying out the review should use their discretion to determine the overall risk level of the organisation, using the criteria only as guidelines.
GMV	See **Legal and Regulatory** impact.
ENISA	Starting from University of Bologna experience, with increasing number of usages it would be possible to consider creating different versions of the ENISA simplified approach for different sectors (University, Public Administration, Private Company, etc.). Even in this case the comments from IAAITC can lead to consensus. The explanation of the productivity criteria/impact in the Risk Profile Selection phase need to be reviewed [2]in order to have a more comprehensive description of a company's risk profile. In the case of Productivity, the impact should be made more comprehensive introducing for example concept like profitability, quality, business process vs. IT dependency, etc.

5.2.3 Financial stability impact

Financial Stability impact	
CESIA	See **Productivity** impact.
IAAITC	See **Productivity** impact.
GMV	See **Legal and Regulatory** impact.
ENISA	See **Productivity** impact.

[2] *As a matter of fact, both comments made by IAAITC are supposed to be part of the Productivity and/or financial stability areas. Both size and turnover of the company have a role in the magnitude of impact. However, their hold true for micro businesses. Turnover is supposed to go hand in hand with profitability and size with the level of liabilities or productivity losses in case of non-availability. Indeed, commented content will be inserted as an explanation to the areas of Productivity and Financial Stability impacts.*

5.2.4 Reputation and loss of customer confidence

Reputation and loss of customer confidence	
CESIA	No relevant comments.
IAAITC	IAAITC argues that whilst the idea of this risk area is valid it can be difficult to assess and quantify. They suggested considering the inclusion of timescales as well as the number of user accesses (i.e. would there be a significant impact on the business if an outage lasted one hour, one day or one month?). When IAAITC presented this topic at events (i.e. specifically for accountants) the responses varied across departments and but also in relation to the period of the year assuming the occurrence of a disaster. So, for example, any form of outage in January (being the peak time in the UK for personal tax returns) is unacceptable to the tax department. On the other hand the payroll departments could accept outages for quite lengthy periods unless it is the last week of the month when the majority of payrolls are run.
GMV	See **Legal and Regulatory** impact.
ENISA	Even though it is always difficult to assess and quantify intangible values, it seems that current definitions for *Reputation and loss of customer confidence* are good and helpful guides for organizations approaching the assessment. Following the suggestion of IAAITC it might be possible to reformulate these definitions including a timescale for availability requirements.

5.3 Critical Asset Identification

In this second phase of the ENISA simplified approach the critical assets of the assessed organisation are identified. These are the assets that are of relative importance to the organization and need to be protected. Together with the critical assets, also the security requirements pertinent to the asset are indentified.

<table>
<tr><th colspan="2">Critical Asset Identification</th></tr>
<tr><td>CESIA</td><td>CESIA proposed adapt in the asset categorisation of “People” and “Application” categories. Those changes/adaptations were made in order to comply with the typical roles and applications used in autonomous University departments. The proposed changes/adaptations are as follows:
<table>
<tr><th>Asset</th><th>Original Classification</th><th>CESIA Classification</th></tr>
<tr><td rowspan="5">People</td><td>Business & HRs Management</td><td>Administrative</td></tr>
<tr><td>Operations & Technology</td><td>Technical</td></tr>
<tr><td>R & D</td><td>Professor</td></tr>
<tr><td>Sales & Marketing</td><td>Researcher</td></tr>
<tr><td>Contractors & 3rd Parties</td><td>Contractors</td></tr>
<tr><td rowspan="5">Application</td><td>Financial Control</td><td>Logistics</td></tr>
<tr><td>Customer Care</td><td>Personnel Management</td></tr>
<tr><td>Logistics</td><td>Fund Management</td></tr>
<tr><td>E-commerce</td><td>Identity Management</td></tr>
<tr><td>ERP</td><td>Career Management</td></tr>
</table>
It is worth mentioning, that such adaptations to the ENISA simplified approach are not only desirable, but also welcome as feedback from deployments of the approach in various sectors.</td></tr>
<tr><td>IAAITC</td><td>IAAICT delivered the comment that this phase works well for larger organisation but it is too complex for micro-business.
Furthermore IAAITC argues that:
• The current structure of the asset selection phase can lead</td></tr>
</table>

	to unnecessary duplication/complexity. • The whole area of networking assets is possibly only relevant for the larger organisation. IAAITC suggests making network infrastructure a single asset option in the (new) infrastructure category and reducing the number of categories. Another point made by the companies involved in the pilot is the lack of focus on soft assets – i.e. the data itself. IAAITC suggests there should be a category or section which focuses on the actual data, procedures for data changing, audit logs of changes, etc. Based on the above, IAAICT would like to consider a more simplified structure for micro-businesses and businesses under 25 employees. The proposal foresees the introduction of six categories for critical assets: 1. **Data storage** – the machines and physical locations where confidential data are stored. 2. **Archiving and Backup –** this includes the method used for backup of confidential data store the backup media. 3. **Connecting Devices –** computers/devices used to access/process data (PCs, laptops, thin clients, PDAs). **4. Staff –** employees and the methods used to access data (s. 3). 5. **(Network-) Infrastructure –** access security and resilience. 6. **Applications –** software used to access data**.**
GMV	GMV has identified several limits in this phase, namely: • A more comprehensive subset of assets. • An analysis of threats and their likelihood of occurrence. • Profiles of potential attackers.
ENISA	• As mentioned in the Risk Profile Selection section, ENISA will consider the possibility to release adaptations of the simplified approach for different company profiles and different sectors. In this respect, different requirements will be taken into account (e.g. business, organisational, resources, etc.). This will be performed by means of pre-assessments.

	• The standard structure for asset classification and identification for Micros proposed by IAAITC it seems to be valid and suitable even if it the need for a thorough review is evident. • The IAAITC suggestion to include Data and Information among other asset categories seems to be appropriate. Corresponding Control Cards need to be introduced as well. • The actual list of assets proposed by ENISA doesn't need to be exhaustive, but it is supposed to be just a support for the non-expert approaching Risk Assessment practice. Users of ENISA supporting material are expected, if it is required, to customize the standard approach to their specific needs. • The introduction of concepts like threats, attacker profiles or even threat frequency and vulnerabilities would certainly make the simplified approach much more complete. However since the whole idea of the "Information Package for SME" was to provide information material for an audience of non-experts, ENISA has to evaluate the trade-off between usability and completeness of the approach before applying any changes.

5.4 Control Cards Selection

In the Control Cards Selection Phase the appropriate controls are identified in order to achieve an adequate protection level (i.e. corresponding to the importance of the business). The controls cards are separated in two categories:

- Organizational controls and
- Asset-based controls

Control Cards Selection	
CESIA	CESIA has made various considerations about organizational control card selection. • SP2 (Security Strategy – Organizational Control Card) was excluded from the selection because CESIA assumed the responsibility of the Security Strategy as their task, centralizing thus the security strategies for all departments. Otherwise CESIA applied the RA/RM approach to different departments as they were different independent organizations, i.e. parts of a federated organisation. • CESIA proposed to include SP1 (Security Awareness and Training – Organization Control Card) in every Risk Area and for every Risk Profile. This is because of the importance the University of Bologna gives to Security Awareness. • CESIA proposed activating control cards for protection of

	workstations even for low risk profiles. This is because they consider this type of asset as the "weakest link" in the entire infrastructure.
IAAITC	IAAITC reported that the idea of using risk profiles and asset identification to select the appropriate cards is a good one and works in a fairly straightforward, intuitive manner. Following the philosophy of critical asset standardization for Micro-businesses, IAAITC suggests that leaving the risk profile as the only variant for the selection of controls would further simplify the process. IAAITC states that for larger organisations, the current process is appropriate and relevant. IAAITC believes also that: • The questions indicated in the approach leading to the selected controls are appropriate. • It is necessary to have an assessor with sufficient knowledge in both IT and business in order to create an appropriate list of control cards. Eventually, some small organisations would have staff with appropriate skills to complete the assessment. • Due to the fact that many small organisations outsource their IT, it would be useful to have a control card related to outsourced services. In the future both Software as a Service (SaaS) and internet services are expected to better penetrate the market of small enterprises.
GMV	GMV has introduced a broader set of Control Cards. They also argued, that some of the proposed Control Cards are not properly described, essentially because they are too long and complex. GMV recommend cutting them into smaller pieces and giving more examples of possible practical application in order to guarantee higher value for SMEs.
ENISA	The pilots confirmed that the use of risk profiles and asset identification to select the appropriate control cards fits well the needs of SMEs. Nevertheless there are some changes/adaptations that need to introduced in order to enlarge the target group of the simplified approach: • Better representation of the Control Cards, by the means of examples (e.g. applicable products that implement a control). • Inclusion of a control card for outsourcing services. • Inclusion of controls for Data and Information protection (Data

	and Information are asset that are missing in the current version of the RA/RM approach). • Clarification of the rule: "the highest risk identified in a risk class defines the overall business risk" in order to reduce costs for the implementation of protection.

5.5 Implementation and Management

During Phase 4, Implementation and Management, the mitigation plan is created.

5.5.1 Gap Analysis

Gap Analysis	
CESIA	No relevant comments
IAAITC	IAAITC highlight that the Gap Analysis process is fairly straightforward. They also proposed to introduce a "traffic light system" to identify gaps based on the following: 🔴 This control is not currently in place 🟡 This control is in place, but needs to be reviewed or updated 🟢 This control is in place and is up to date
GMV	GMV, borrowing a feature from the Pilar tool, introduced the concept of CMMI in the Gap Analysis. Five levels of compliance are defined plus a level 0 (Non Applicable) in the case the Control Card does not apply to the specific context. Apparently, these compliance levels are compatible to the Capability Maturity Model (CMM). • L0. Non Existent: the safeguard is not even regarded, nor set. • L1. Initial /ad hoc: The safeguard is not set, but is regarded, planned or partially set. • L2. Reproducible but intuitive: The safeguard is set but not under a clear procedure. • L3. Defined procedure: The safeguard is set and there is a clear procedure, with documentation. • L4. Managed and measured: The safeguard is set, has a clear and documented procedure and its presence and efficacy is measured and controlled. • L5. Optimized: All the points in L4 plus optimized, meaning that after measurement and control it has been improved to its maximum efficiency.

ENISA	The introduction of the "visual approach" suggested by IAAITC is a good idea, since it makes the gap analysis easier and more intuitive. The viability of CMMI approach needs to be further investigated. As both proposals are leading to diverging degrees of complexity for the simplified approach, ENISA plans to find a solution towards a balanced average approach.

5.5.2 Mitigation Plan

Mitigation Plan: Creation-Implementation-Monitoring -Control	
CESIA	No relevant comments
IAAITC	No relevant comments
GMV	No relevant comments
ENISA	No relevant comments

6. Concluding Considerations

The validation of the simplified RA/RM approach using pilots was the second stage of the ENISA's initiatives to promote Information Security Risk Management. The objectives of the pilot projects were:

- validation of its applicability,
- generation of awareness among the involved multiplier organisations,
- the assessment of impact that could be reached with the Information Package for SMEs and,
- the improvement of simplified approach based to feedbacks from pilots.

Apart from the challenges faced in the performance of the pilots with very small businesses (i.e. micro enterprises), the results are rather encouraging especially as far as the impact of the Information Package for SMEs is concerning. In cases where the risk assessment has been outsourced to experts, the simplified approach demonstrated its merits from the point of view of simplicity and usability of the achieved results. According to the reports received after the pilots, there was a generally high level of appreciation for the information material provided by ENISA.

The clear message received from the pilots is that the direction undertaken by ENISA is the right one. Since SMEs are too busy dealing with their core operational activities, they need to be encouraged to focus on other priorities, they need to be guided in the process of change and they need to be supported with the right tools.

Quoting, for instance, a questionnaire from GMV, the SMEs participating in the project are now more motivated to improve their information security management approaches (the qualitative response was 4.33 out 5).

However, challenges related in-sourcing of the simplified approach within SME and Micro Enterprise (ME) environments have been faced. Some of the challenges were, for example, the lack of understanding of the importance of protecting their information, intellectual property and know-how, the shortage of resources and expertise, the misunderstanding of the Risk Management concept and, from the operational point of view, the misalignment between Boards of Directors (entrepreneurs) and IT departments (technical staff).

All these issues, also identified by the ENISA Ad Hoc Working Group on Micro Enterprises (see Final Report of the Working Group), were confirmed by the multipliers involved in the pilots.

Regarding the applicability of the Information Package for SMEs, received feedback was consistent; in the message was that the approach is straightforward, but it is unlikely that SMEs and MEs (especially small and micro enterprises) could use the simplified RA/RM approach as such, without an external support, at least in the first implementation. As a matter of fact, all the organizations in the pilot chose the outsourcing option.

On the other hand, ENISA's strategy to give to multiplier organizations a key role in the pilot was correct, but it also became evident that their involvement in information security awareness raising process must increase. The need to involve relevant stakeholders and multipliers has been confirmed by the Group of Expert members of the Ad Hoc Working Group Micro Enterprises.

Another interesting conclusion that has been also identified by the Working Group is the necessity to deepen the dialogue with multipliers in order to find deployment strategies for such material. It seems that besides the content, the strategy to generate incentives and awareness for the potential recipients of such approaches is a key issue for success. It is necessary to investigate possible schemes to enable the participation of SMEs in such information security activities.

Equally interesting feedback related to the approach has been gathered from the pilots. The different geographical distribution and market sector of the companies involved in the projects as well as the different information security penetration level in their countries of origin, allowed ENISA to collect a wide variety of different perspectives on the Information Package for SMEs.

The most controversial phase of the simplified RA/RM approach was surely the Risk Profile Selection, but even for the Critical Asset Identification and Control Cards Selection phases many comments were collected.

The areas of risks taken into account in the Risk Profile Selection Phase consider a broad range of possibilities but there are still some gaps to address in relation to both the description of risk areas and other/alternative qualitative criteria that could be used in order to assess the risk profile of organisations. For instance, IAAITC pointed out that some areas of risk, namely Productivity and Financial Stability, need to be reviewed to reach a more comprehensive and precise description of a company's risk profile.

Furthermore, a call for simplification and customization was made by all the multipliers, especially the ones related to micro enterprises. As regards the first aspect, the introduction of questionnaire-like approach was suggested (by GMV), whereas UNIBO and IAAITC proposed respectively a sector-based and market-based approach.

The same clear request for a more streamlined and tailored approach comes from the comments related to the three other phases of the simplified RA/RM approach for SMEs.

In conclusion, the simplified RA/RM approach for SMEs is a useful support for small and medium enterprises with a minimum level of understanding about IT and Information Security, but it doesn't scale down sufficiently to fit the needs of very small and micro organizations. Some minor changes would enhance the value of ENISA's information material for small and medium enterprises, whereas bigger changes are required in order to increase the benefit for very small and micro enterprises. An automation of the phases by means of a tool might bring the desired simplification. Another possibility which will be taken into consideration is the generation of a set of assessments covering different types of (micro) enterprises. In this way, interested parties can choose among a set of assessments based on their size and type of business.

7. Road Map for improvement

ENISA will put in place a medium term plan to improve the Information Package for SMEs.

Starting from comments, suggestions and ideas raised from the organizations involved in the Pilots, ENISA has identified areas for future development of the simplified approach.

Changes in terms of the structure of the approach as well as in terms of content will be introduced.

In the short term the Agency will focus mainly on revisions of the content. The following changes will be implemented:

1. Review of questions for Outsourcing Options selection.
2. Review of Legal and Regulatory Risk Area definitions.
3. Review of Reputation and Loss of Customer Confidence Risk Area definitions.
4. Review of Risk Profile selection rule.
5. Review of Critical Asset Categories.
6. Review of Control Cards to introduce threats and examples for their implementation (e.g. through existing products).

7. Improvement of the gap analysis.

Furthermore, the Risk Profile Selection Phase will be reviewed. The objective is to learn from the obstacles encountered by the SMEs in the Pilot and make the task clearer and more straightforward.

The results will better address the need of small and medium enterprises.

In the short/medium term also some more structural changes will be also applied.

From the structural point of view, two main adjustments are under evaluation.

The first one consists in the creation of a specific Risk Assessment and Management approach for Micro Enterprises.

The second one stems from the suggestions from both the University of Bologna and IAAITC and it concerns the possibility to release different approaches to address the requirements of businesses in different sectors (PA, University, Private Sector, etc.) and in different markets (i.e. market with specific regulations).

The limited resources available won't allow ENISA to deliver distinct and structured methods addressing the needs of different sectors/markets. Due to these limitations, a more realistic approach will be the inclusion, (i.e. in the form of annexes to the standard simplified RA/RM approach) of customized contents (i.e. special control card for each sector, different areas of risks, etc).

As the University of Bologna pilot has shown, the most efficient and effective way to produce special content tailored to a specific sector is to collect feedback from real world implementations.

That means that the ENISA will call for collaboration any European organization willing to apply the simplified RA/RM approach and to customize it for their specific needs.

Finally, by means of a work package that is foreseen within the ENISA Work Program 2009, ENISA is going to generate documentation on the simplified approach by including awareness material. This will be performed together with a multiplier organisation. Objective is to generate a "glossy" version of the simplified approach that can be directly disseminated via professional associations and other interested organisations.

8. References

[1] Information Package for SMEs – ENISA

[2] Final Report – ENISA Ad Hoc Working Group on analysing micro enterprises' needs and expectations in the area of information security

[3] Basel II Accord – International Convergence of Capital Measurement and Capital Standards, Basel Committee on Banking Supervision, November 2005

Annex A: Feedback from UNIBO

Feedback by the University of Bologna on Risk Profile Classification and Organizational Control Card Selection in the application of OCTAVE method for the Academic environment

1.A Introduction

The University of Bologna is one of the important academy institutes in Italy with a large number of students, scientific/cultural activities and with a lot of relationships with industries and companies that confirm the relevant role that the university has reached in the last century. Today Bologna is proud to guess an academy institute with a high-specialized administrative/technical staff for offering quality services to academy's best customers: the students.

The most important roles is play by Center for the Management and Development of Services (CESIA) that is responsible for the most important service as: (a) the academic network connection to Internet, (b) the official email service @unibo.it, (c) the hosting of the academic portal web site, (d) development and hosting of dozen of software applications for the administrative areas.

In the last two years another hot topic is faced by the technical staff: How to improve, or create, the security process regarding people, systems and information?

But if CESIA wants to face this challenge it's important to give the dimensions of the problem: 90.000 active students, 12000 administrative/technical/research staff, 90 departments and 20 faculties; and what about the incidents: in 2007 first quarter about 200000 events categorized as high risk by Intrusion Detection System, and in 2007 second quarter about 600000 events categorized as high risk; and in case of compromised host the incident is caused by: the 40% of host is victim of botnet IRC, the 30% of host have no kind of protection as personal firewall or antivirus (if there is one, maybe is not updated) and the remaining 30% has an operative system with no updates and hotfix.

The way used by CESIA to face security for whole academy can be separated in two ordered and distinctive levels: reactive e proactive.

The reactive part is built principally of a brand new group in CESIA called Security Team that constitutes the Computer Emergency Response Team (AlmaCERT). AlmaCERT is responsible for management of intrusion detection system and alarms deriving from it, forward alarm to departments and faculties, manage incidents in collaboration with national/international security teams, implement and deliver proactive service as centralized antivirus platform (based on a commercial software), and centralized windows update system for updating clients and servers.

The proactive part is built on a project called "Risk assessment and management in academy's structure" and is based on the ENISA deliverable "Information Package for SMEs". The ENISA document on the Risk assessment and management for SMEs should be adapted in case of academy environment.

CESIA and the University of Bologna will provide for ENISA the possibility to extend organizational control cards and asset control cards in an academic network. The main challenge is represented by the fact that in an academic network it is rather unlikely to find equity between research activities (and its natural attitude to experiments and loss of rules and limits) and information security (that is based on the assumption of limitation imposed to use of technological assets and treatment of data and information).

The first objective is to enhance the security level of departments thanks to a standard methodology provided by ENISA. In fact, the "Information package for SMEs" contains a risk assessment/risk management methodology which can be used in case of small, medium and big departments (all of them can be treated as a SME),

The second objective is to focus on a risk profile evaluation table. CESIA wants to give ENISA a feedback in order to rewrite this table when the SME objective of risk assessment project is a PA department. As a matter of fact, "legal and regulatory", "productivity", "financial stability", and "Reputation and loss of customer confidence" and their definitions for a classification in high, medium and low classes are not so appropriate in case of a PA. For example "financial stability" for an almost useless department since its budget depends on general administration of University of Bologna. CESIA wants to rewrite this table, changing the risk areas ("legal and regulatory", "productivity", "financial stability", and "Reputation and loss of customer confidence") and the definition for classifications. Of course, CESIA wants to give indications and suggestions on the appropriate organizational control card selection.

2.A Methodology related issues

This chapter will discuss any single aspect emerged in the application of ENISA deliverable "Information Package for SMEs" to departments of University of Bologna.

Decision makers and outsourcing

Who are the decision makers? In this project are the department's councils and their directors. These staffs are well informed on any single phase regarding risk analysis and risk assessment project, and they have to approve changes from the analysis phase to the implementation of security measures.

The working staff model is based on partial outsourcing and it assumes that the initial risk assessment is provided by CESIA (that is responsible for the whole academic IT network infrastructure), that acts as an external company from the departments point of view. Also, the initial assessment provides knowledge transfer to the department internal personnel. Finally, the implementation phase is performed by CESIA in collaboration with local technicians.

Risk profile selection

Statement of application

The main problem faced is related to the risk areas in the table of risk profile selection due to the different economical and organizational nature of a department with respect to a SME.

These are the main considerations on risk profile selection:

- The first and the last risk areas, **Legal and Regulatory** and **Reputation and loss of customer confidence** can be easily used for a department. In fact, a department usually manages personal and medical data for research activities. If customers' role is substituted by students is easy to understand why a department has to maintain a correct level of reputation.
- The second and the third risk areas, **Financial Stability** and **Productivity**, have to be modified. A department's financial stability depends on the economic stability of the whole university and, of course, it is more stable than a SME. Departments' productivity can be split in two main areas because a department can be viewed as a very specific SME dedicated to teaching and research.
- If it is not possible to establish the correct profile risk, it is also impossible to use the organizational control cards selection table. This kind of selection is very important to establish a security treatment for the whole organization. The

paragraph below shows the right connection between the new risk areas and the organizational control card provided by OCTAVE

Modifications proposed

The main change is dedicated to risk selection where "Financial Stability" and "Productivity" are replaced by:

- **Teaching**: this is the main common and important activity of departments. The risk is high if the unavailability of one of the above services can stop one of the teaching activities and/or if it can cause the loss of data and information related to examinations or student's careers,
- **Research**: this area has a strategic role for many departments and especially for those that are based on their academic prestige on the quality of their research. The research can be classified as a high area risk if the unavailability or the incorrect management of this area (for example, unavailability of laboratories and devices, lack of international relationship, lack of knowledge about fundraising) can have a direct impact on this strategic activity.
- **Patents**: research activities can produce a very specific technological knowledge and, sometimes, these activities can be registered as patents. Patents can lead to economic benefits to support research, international academic prestige and/or collaboration with companies.
- The table below shows the modification to table 2 about the ENISA's deliverable "Information package for SMEs" (paragraph 4.3.1, Phase 1 – Risk Profile Selection pp. 20).

Area Risk	High	Medium	Low
Legal	The organization handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	The organization handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	The organization does not handle personal data other than those of the people employed by the organization.
Teaching	**Unavailability or Service Quality directly impact the teaching**	**Unavailability or Service Quality can**	**Unavailability or Service Quality have**

	activity of department (laboratories, libraries, technological classrooms, reservation of classrooms, reservation of examinations, registration of examinations, students activity)	**indirectly impact on teaching activity of department**	**no impact on teaching activity of department**
Research	**Unavailability or Service Quality directly impact on research activity (laboratories, IT classrooms, libraries, fund raising, international relationship)**	**Unavailability or Service Quality can indirectly impact on research activity**	**Unavailability or Service Quality have no impact on research activity**
Patents	**An infringement of patents will cause the loss of economical benefits and th loss of technological knowledge with respect to competition**	**An infringement of patents may cause the loss of economical benefits**	**the department has no registered patents**
Reputation	Unavailability or Service Quality directly impact the businesses of the organization or/and more than 70% of customer base has online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/or less than 5% of customer base has online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

Table 1: Risk profile selection

Critical asset identification

Statement of application

The asset identification remains unchanged because the definitions relating to systems, network, people and applications are suitable also in the case of

departments. Only a modification to the examples of assets related to people and applications was required.

Modifications proposed

There are modifications proposed to people and application categories in order to be compliant with typical roles and software application used in a department:

Asset	Description	Asset type
System	Information systems processing and storing information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered as a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings; those that store critical business information (customer or business proprietary) or those that are exposed to the outside world for business functions or services.	Server
		Laptop PC
		Workstation
		Archiving and Backup
		Storage
Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of components. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with a third party and usually untrusted networks	Routers
		Cabling
		Gateways
		Wireless Access Points
		Network Segment (e.g. cabling and equipment between two computers)
		Firewall
		VoIP
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes.	**Administrative**
		Technical
		Professor
		Researcher
		Contractors
Application	Critical Applications. Applications that are key to or are part of the product and service offerings. The disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	**Logistics**
		Personnel Management
		Fund management
		Identity Management

		Network Services Management
		Career Management

Table 2: Asset category classification

Organizational control card selection

This is the second main modification to ENISA's deliverable (Phase 3 – Control Cards Selection, section Organizational Control Cards Selection, table 6.

Statement of application

- The organization control card dedicated to security strategies (SP2) is not present in table 3 "organizational control card selection", because CESIA has centralized the security strategies for all departments. In fact, security strategies cannot depend on single departments, and furthermore this avoids that the choices made by departments vary between structures
- The organizational control card dedicated to Security Awareness and Training (SP1) is present everywhere in table 3, since security awareness and training is considered as the most important step in security risks mitigation, and it is supposed that teaching activities can be organized into an appropriate manner
- According to the academic security strategies and policies, it is important that control cards for the protection of workstations (SP4) are activated even if the department risk profile is classified as low

Modifications proposed

These changes cover all areas, both the changes relating to legal and reputational, and the new areas previously introduced (research, teaching and patents).

Risk Area	High	Medium	Low
Legal	**(SP1)** **(SP3)** **(SP4)** **(SP5)**	**(SP1)** **SP3.2, 3.3, 3.4** **SP4.1, 4.2, 4.3, 4.6** **SP5.1, 5.5**	**SP1.1** **SP3.2, 3.4** **SP4.1, 4.6**
Research	**(SP1)**	**(SP1)**	**SP1.1**

	(SP3) **(SP4)** **(SP5)** **(SP6)**	**SP3.1** **(SP4)** **SP5.1, 5.2, 5.5** **(SP6)**	**SP3.2, 3.4** **SP4.1** **SP5.1**
Teaching	**(SP1)** **(SP4)**	**(SP1)** **(SP4)**	**SP1.1** **SP4.1**
Patents	**(SP1)** **(SP3)** **(SP4)** **(SP5)** **(SP6)**	**(SP1)** **SP3.1, 3.5, 3.6** **SP4.1, 4.2, 4.6** **SP5.1, 5.2, 5.5** **(SP6)**	**SP1.1** **SP4.1**
Reputation	**(SP1)** **(SP6)**	**(SP1)** **(SP6)**	**SP1.1** **SP4.1**

Table 3: Organizational control card selection

Implementation and Management

The project execution requires a good IT expertise level; usually, these skills are not found in IT departments. That is why CESIA has included a training phase for IT personnel to the project. The aim is that of creating a centralized management of technicians who may be located in a dynamic way through various departments.

Final considerations

CESIA was responsible of the editing of some parts of the ENISA deliverable in order to make it suitable for the academic departments. In particular, the editing was focused on risk profile selection and organizational control card selection.

All the other parts remained unchanged, such as any single asset control card, any single organizational control card.

From our experience emerged that the ENISA deliverable is good risk assessment and risk analysis base for the academic environment and fitted the University of Bologna needs with just slight modification to risk profile selection and control card selection.

3.A Future works

We suppose that the introduction of a scale for classifying the security level of any single department should be a good idea. This scale is designed to create a sort of ranking for departments. The ranking is updated at any periodic verification of the department's risk profile.

The number of risk areas could be updated by increasing the number of departments, or expanding the project to academic structures (for example, specialized master schools, interdepartmental centers, etc) that have different needs with respect to individual departments.

After implementing the project security in a sufficient number of departments, training courses will be activated to increase the level of information security knowledge among technicians.

The security project provides a phase dedicated to collaboration with other Italian and European universities to exchange information on projects similar to those at the University of Bologna.

The part of the asset-based control cards could be modified for a larger adaptability to the case university, but currently this is not a significant change and improvement for the project. It could still emerge only after an enlargement in terms of nature and number of facilities which the university involves.

Annex B: Feedback from IAAITC

International Association of Accountants
Innovation & Technology Consultants

ENISA Risk Management
Pilot Study - 2008

Executive Summary

Four Member Firms of the IAAITC conducted pilot studies on a number of their clients using the ENISA Risk Management Methodology.

The material used was the ENISA deliverable of 2007 as subsequently amended by the IAAITC to produce a card set colour coded as high /medium / low risk (red / yellow / green).

The same colour coding methodology was used in the preparation of the reports:

Red = item was of high importance and required immediate attention
Yellow = item was of importance and would require attention
Green = complied or was irrelevant

6 businesses (client firms) of differing business types /sizes completed the pilots.

Pilot No	Business Type
1	Accountants
2	Training College (Journalists)
3	Scientific Membership Society
4	Event Management
5	Financial Services
6	Physiotherapy Services

Examination of the Pilot Reports will show that issues were easily and quickly identified:

Pilot No	Risk Profile	No of Red Issues	No of Yellow Issues
1	High	11	7
2	Medium	8	12
3	Medium	6	4
4	Medium	6	6
5	High	4	0
6	High	13	10

Having conducted these pilots we would conclude:

- The ENISA methodology is effective at quickly identifying the relevant issues across businesses from a number of sectors.
- Some familiarisation is required if a consultant is going to use the methodology and material, but this is minimal.

- As the material stands at the moment micro businesses would be unlikely to conduct their own self assessment and are unlikely to be prepared to pay a third party to do it.
- Some customisation / simplification of the material would be of help in rolling it out at the micro and small business level.

1.B Introduction

Background Information

The IAAITC had commenced working with the ENISA deliverable on Risk Management in 2007.

Following the broad concepts as we understood them we developed what is effectively three sets of cards the controls being colour coded red / yellow / green:

- The four step methodology
- Organisational Controls
- Asset Controls

During the later part of 2007 the IAAITC with a number of firms ran some pilot workshops on the topic of Risk Management. These were to general audiences and we found that trying to address businesses of different types and sizes together did not work effectively as it was very difficult to get the level right. Micro businesses did not necessarily accept that they could be HIGH Risk, and larger businesses sometimes felt they should be HIGH when in reality they were not.

During 2008 the IAAITC has run some workshops specifically for Accountants. Using the material as it stands with an audience from one sector is a lot easier. Initially the material was delivered and the delegates were encouraged to reach their own conclusions. More recently we have amended the format so that for example rather than asking them to decide if they are HIGH risk, we tell them that they are and explain why. This approach allows more time to be spent on the controls.

The material could be improved further for this sector which is something we would like to consider with the help of ENISA during 2009.

Scope and objectives of the pilots

It was agreed with ENISA that a number of IAAITC Member Firms would conduct pilots within their client base. Being Chartered Accountants, with an understanding of audit principles it was felt that accountants would be a possible channel for delivering this material particularly in the micro and small business sectors which tend not to be addressed by the IT industry.

The objective was to conduct 5 Pilots.

The firms selected were from different parts of the country and they were allowed to choose the client(s) they used. They were asked to nominate a number of clients and the final selection was made to ensure that different industry sectors and size of business were involved.

The objectives were as follows:

- How easily could a third party (in this pilot - accountants) grasp the concepts and understand the methodology.
- How effective was the material when used across businesses of different sizes and types.

2.B Selection of firms and deployment of pilots

Selection of firms

A number of Member Firms were given the opportunity to become involved in the exercise. The only criteria being that they had a familiarity with IT, which all members of the IAAITC inevitably have, and a familiarity of audit procedures.

The familiarity with audit had an interesting implication which we failed to consider. Whilst all accountants will be familiar with audit and have done some during their training not all follow this discipline once they qualify.
Where we had a member who was still involved in audit and up to date with current methodology to international accounting standards we encountered some interesting issues. Financial Risk being a topic covered in audit meant that he had slightly different views on how a business should be profiled.

Approach followed in the deployment

Although five IAAITC Member firms were engaged to conduct pilot studies, in the end only 4 completed the pilots within the required timescales. Only 6 pilots have been done in total.

The material that they were given to use was the material produced by the IAAITC from the ENISA deliverable last year.

The Member Firms were briefed together on the material, although all had already seen it in a workshop environment. The four step process was explained although

they were specifically briefed on a preferred methodology for delivering the material. It was expected that they would in view of their general professional and audit experience all approach the task the same way, which with some minor exceptions proved to be the case.

The Firms, conducting the pilots, all of whom are Chartered Accountants who position themselves as Business Advisors were:

Firm	Location
RMT	Newcastle upon Tyne
WKH	Letchworth
PEM	Cambridge
Morris Owen	Swindon

In selecting the Clients it was agreed that we should endeavour to select businesses that were typical and not geographically specific for this exercise. Our justification for this being if we choose typical businesses then in future there would more possibility in extending the reach for deployment.

So for example there are accountants in every town and city in the UK, similarly there are various types of training /membership establishments / or medical services.

Certain business types are more geographical located. Whilst it would have been interesting to do some work in say the tourist industry we have to accept that in the UK that industry is confined within fairly clear regions.

The business types chosen were therefore thought to be relevant to all parts of the country.

Pilot No	Business Type
1	Accountants
2	Training College (Journalists)
3	Scientific Membership Society
4	Event Management
5	Financial Services
6	Physiotherapy Services

Validation of the pilots

We have since the beginning of 2008 been working with the School of Computing, Engineering and Information Sciences of Northumbria University. The University was extremely impressed with the ENISA material and the IAAITC treatment of it. They will shortly commence validating the pilot studies as a separate exercise.

3.B Comments and issues identified

Basic Approach

The simplified approach of the 4 step process works extremely well. The concept of the cards is generally good.

From our experience inevitably we feel that there are some areas where more detail is needed and others where less complexity is required. We do however accept that this is a limitation of trying to create generic material.

It is worth noting that one firm although only required to do one pilot, actually did 3 because they **wanted** to and is now waiting to be told what to do next!

Outsourcing Options

This section could be simplified and there are issues in the questions asked.
If for example we are dealing with micro businesses, asking if they can make available two to five people for the project is probably not an appropriate question. There are also issues over the wording although this is probably a translation issue for example. "Does your business and service offerings include financial transactions?" is basically asking do you sell any goods and services. What we suspect is meant by this is "Does your business and service offering include financial services?" such as those regulated in the UK by the FSA.

We would consider a simpler breakdown – which should be along the lines of:

- Do you have the time available within the organisation to carry out this review?
- Do you have the knowledge available in the organisation to carry out this review?
- Do you want an external assessment of your Risk Management position?

Based on these questions a business should be able to decide whether they wish to carry out the review in-house, outsource all of the review to an external assessment body, or a combination of the two.

Another possible option is to award points to each question and introduce an element of weighting – as in a survey. i.e. On a scale of 1 to 10 – rate your IT knowledge. The decision on whether to outsource can then be based on the overall score.

This would also enable a simple web based survey to be built.

Risk Profile selection

Legal and Regulatory

The sensitivity of the data held focuses on the data of third parties. Many organisations hold information on their own organisation, products and services which would also represent a major business risk if accessed by unauthorised people. Examples include all forms of Intellectual Property, such as product information for technology companies.

The criteria for this profile could be based on asking the business to identify what they consider the key information held, and then assigning a risk to that data being lost or disclosed to unauthorised people.

Productivity and financial stability

Basing the risk purely on financial turnover or number of employees possibly allows scope for error. The turnover is irrelevant in terms of the level of risk, and risks confusing the issue. The number of employees is useful for giving an idea of the number of contact points, but again this does not take into account the type of business.

A number of the pilot businesses felt that this seemed to bias the survey to small organisations being low risk, whereas in many cases this would not be true.

Also the financial criteria listed have a gap between the medium level (up to £6M) and the High level (over £15M) which needs to be corrected. (This is as a result of us setting the medium level to coincide with the audit threshold. Accountants will view businesses where they are doing a statutory audit slightly differently from businesses where no audit is required.

Reputation and Loss of Customer Confidence

Whilst the idea of this risk area is valid it can be difficult to assess and quantify. We could consider including timescales as well as amount of user access. i.e. would there be a significant impact on the business if an outage lasted one hour, one day or one month? (When we covered this topic at events specifically for accountants the responses varied across departments and the time of year you selected to have a disaster. So for example any form of outage in January which is the peak time in the UK for personal tax returns is unacceptable to the tax department, but the payroll departments could accept outages for quite lengthy periods unless it was the last week of the month when the majority of payrolls are run.)
The other point that needs emphasising is that these are guidelines and not necessary to be taken literally. Any financial criteria need to take into account the business type – a small car dealership may have a very high turnover because it deals in high value goods, but an accountancy firm may have limited turnover because the only sales are service costs. In short – the person carrying out the review should use their discretion to determine the overall risk level of the organisation, using the criteria only as guidelines.

Asset Selection

This whole section works for larger organisation but at the micro-business level it adds an extra level of complexity.

For Micro-businesses and businesses under 25 employees we would consider a more simplified standard structure. This would still encompass the main typical assets but provide a simpler structure for people to follow.

We would consider basing it on the following six assets:

- Data storage – the machines and locations where you hold your data.
- Archiving and Backup – how you back up and keep protect your information in case of loss.
- Connecting Devices – machines used to access data (PCs, laptops, thin clients, PDAs).
- Staff – your employees and how they access information.
- Infrastructure – access security and resilience.
- Applications – software used to access data.

The current structure of the asset selection can lead to unnecessary duplication. An example of this is where an infrastructure asset is selected; there are numerous questions on data backups. However you also have the ability to select "Archiving and Backup" as an option in its own right. This effectively gives duplicated questions, and also leads us to ask – do you back up your backups?

The whole area of networking assets is possibly only relevant for the larger organisation. There are fewer points of risk associated with these in a small business and arguably are much lower than the other three asset categories. We would therefore suggest making network infrastructure a single asset option in the infrastructure category and reduce the number of categories to three.

One point made by the clients was the lack of focus on soft assets – i.e. the data itself. Perhaps there should be a category or section which focuses on the actual data, procedures for data changing, audit logs of changes, etc.

Card Selection

The idea of using the risk profile and asset identification to select the appropriate cards is a good one and works fairly straightforwardly. We would certainly recommend that this process is carried on going forward.

As above – for Micro-businesses we would suggest standardising the assets so that the only variant is risk profile, as this would simplify the process for them. For larger organisation the current process is appropriate and relevant.

Alternatively we could consider just apply the simplified asset selection process to organisations with a Low or Medium risk profile, whilst those of a high risk do the full asset selection process.

Card contents

Generally these are appropriate and produce valid questions for the organisation and assets concerned. The structured layout makes it fairly easy for the assessor to identify the questions to be asked. There is still, however, the need for a degree of discretion on behalf of the assessor to ensure that inappropriate questions are not asked.

There are a number of controls that refer to more technical questions, and therefore it is necessary for the assessor to have a certain level of technical knowledge. We believe that for the assessment to have validity it will be necessary for the assessor to be sufficiently knowledgeable in both IT and business. Few small organisations would have staff of appropriate skills to complete the assessment.

The cards make no allowance for the provision of outsourced services. Many small organisations outsource their IT support and maintenance to third parties, and many of the questions focus on the controls for internal staff. With the expected increase of SaaS, and internet services generally perhaps a separate set of cards could be produced focusing on the provision of outsourced services.

(We have for example come across organisations offering hosted services and whilst the servers may be located in a secure environment (by no means the norm) the associated administration procedures leave much to be desired.)

Gap analysis

Going through the controls to identify what is currently in place and what gaps exist is fairly straightforward. The general consensus amongst the Member Firms was to use a traffic light system to identify current gaps based on the following:

Red	This control is not currently in place in the organisation.
Orange	This control is in place, but needs to be reviewed or updated.
Green	This control is in place and is up to date.

This then provided a simple checklist from which the client can see the actions they are required to take.

4.B General Findings

Our general conclusion is that this methodology works well for companies of a certain size, which would have the resource to do it themselves, but does not scale down sufficiently to provide a suitable framework for micro organisations. These organisations require a simpler framework that can be processed more quickly and with less outside input.

For micro businesses we consider that the Asset Selection could be simplified and probably based on 4 levels of technology assets.

- Stand alone PC
- Multiple standalone PCs
- Peer to Peer Network
- Single Server Network

We also feel that if variations of the material which were sector specific were developed it would be easier to deploy. The Institute of Chartered Accountants of Scotland (ICAS) has expressed an interest in the possibility of being involved were we to develop material specifically for the accountancy profession.

The likelihood is that other bodies / membership organisations would also be interested if material was available for their specific sector.

1. In general all of the firms are pleased with the deliverable, and would like to see further developments.

2. A general point is the English, whilst we know what you are trying to say, will the small businesses or will other countries where English is not their first language be able to translate into their own native language accurately. We think some work needs to be done on refining the language in some areas.

3. One of the major points to consider is - who is the targeted audience for this material. None of the accountants think that the micro businesses would have the resource or skills to do this themselves, and most would not see a value in paying a third party. There are potentially going to be problems with terminology if we stick to the business sizing according to European guidelines. There are plenty of micro organisations with turnovers of less than 1million, which should be high risk but could classify themselves as low given their size and turnover. Perhaps some of the most obvious examples are small firms of accountants or lawyers.

4. One consideration would be to target the regulated industries with a more specific selection of the material.

5. The review works well for larger organisations where the client is able to devote some time to the project and/or is prepared to pay a fee for an assessor to carry out the review for them. In the case study of a 150 employee firm the project would therefore be seen as a feasible and worthwhile project.

6. For a smaller organisation, such as the case study of 15 employees, the process is too complex and time consuming given the level of value the client would put on the project. They would not have spent the time using in-house resource to complete the project, and given the time involved the price of this survey from a

third party would have been in the region of £500 - £750 for their organisation. Whilst they benefited from the results of the review, in a commercial setting where they were paying for an assessor they would probably have chosen not to go ahead.

7. If the packs had been sent out to the pilot clients, they would possibly have tried doing it themselves as they had already been briefed by the accountant. But if it is generally made available to businesses there needs to be a point of contact for them if they have any questions or require further assistance. Obviously this is a role the IAAITC members could look to cover on a regional basis.

Annex C: Feedback from GMV

Risk Management Pilot for SMEs and Micro Enterprises in Spain

Final Report

Executive summary

The RM Pilot for SMEs and micro-SMEs in Spain has given the opportunity to all participants to start using the simplified Risk Assessment and Management approach described in the ENISA deliverable: Information Package for SMEs – Please see References Annex for further information about this Package.
Most of the Risk Management experiences in Spain come from the Official organizations, who rely on Magerit Methodology. This is also the methodology of reference for most of the biggest companies, as they usually collaborate with the Administration.
However, there was no tool available or at least not recommended for Small and Medium Enterprises. As a consequence of it, most of them did not know how to take decisions related to investment in IT Security.

As this report is intended to explain in detail the RM Pilot in Spain, it will start telling the reasons that moved both ENISA and rest of participants to go on with this project.
Then, it will be described the criteria followed for SMEs selection, including a brief description of each SME and the characteristics that made them valuable for this RM Pilot.
After this introduction, it will be shown the activities accomplished and developed of the Pilot in terms of meetings, follow-up actions and progress schedule.
It is also offered information from Workshops held within this Pilot and another related dissemination activities such as ENISE Workshop.
Another issue of great importance dealt in chapter 3 is related to the Methodology deployment over the Pilot. It is explained the reasons for the choices made in order to fit both to the characteristics of the enterprises but also to the RM tool used.

In chapter 4 it is discussed in detail the troubles found using ENISA Methodology approach and it has been suggested a number of modifications regarded as of interest.

Results of the Pilot in are presented in chapters 5, 6 and 7. First it comes a general overview of the experience from GMV's point of view as RM outsourcers and then there come the comments made either explicit or implicit by SMEs and rest of participants – RM tool provider, CEEI and overall comments taken from workshops.

Chapter 7 is devoted to Feedback from companies, which is the most interesting result of the report and measures the satisfaction obtained by SMEs and micro SME involved. It is included a review of comments translated to GMV and regarded of interest.

Finally, the working documents used within the project – Questionnaires, RM reports – Sanitized due to Non Disclosure issues with SMEs involved – are presented here.

As an overview of the findings of this pilot, here are the most important points dealt throughout the last chapters:
SMEs take decisions related to technical solutions implementation mainly using a cost-benefit analysis of safeguards. They usually think only on a near

future scope and focusing only on understandable and really very provable threats. This analysis is not currently managed by ENISA approach.

SMEs try to save as much money as possible when looking for safeguards implementation. So they demand help in finding costless or very cheap solutions, which is out of the scope of the methodology approach.

We consider that Risk Management tasks should be complemented with these two key elements:

- Previous widespread awareness of Board of Directors of SMEs on Risk Analysis and Risk Management no matter the methodology applied.
- The RM report should be accompanied by a guide on how to implement safeguards.
- A set of references and documents and websites of interest to enhance their knowledge about RM but also about security best practices.

1.C Introduction

Background of the pilot

Over the last ENISA's event on Risk Management that took place in Barcelona, November 2007, it was highlighted the lack on Risk Management culture among Small and very Small enterprises.
There was also reported the absence of motivation in introducing IT security and Risk Management and requested targeted activities to enhance this ground on IT security for small and micro enterprises.
Despite some reports that echo an increasing investment in technology by Spanish companies and a reasonable concern about security measures to protect their business assets, it is clear that most companies, specially the smaller ones, are not used to Risk Analysis, Business Impact Analysis or in some cases any Analysis at all. That means that they are purchasing security solutions in blind fashion.
In its efforts to promote Risk Management and Information Security, ENISA has generated a methodology approach based on OCTAVE, aimed to help small enterprises (SMEs) to understand and to apply Risk Management. (See ENISA Deliverables mentioned in the References chapter: "Information Package for SMEs" and "RM&IT Security for Micro and Small Business·

Objective of the Pilot

One of the major ENISA's goals is promoting the Information Security Awareness.
In order to achieve this objective, ENISA Work Program for 2008 has included a preparatory activity with the title "**Building Information Confidence with Micro Enterprises**".
Within this activity, it was regarded a number of pilots (initially four) to be performed during present year to check the applicability of available ENISA results in the area of Risk Management for Small and Micro enterprises.
With these pilots ENISA would like to promote Risk Management among this type of enterprises.
The pilot was regarded to be performed in cooperation with a promoter organization that should guarantee the incorporation of a potential set of small and micro enterprises.
In our case, the CEEI – That stands for Center of European Enterprises in Castilla-Leon area – was contacted by GMV to participate in the Pilot.

The industrial team participants showed **different interests and motivations for participating in the pilot:**
GMV, as a professional services firm in the information security industry, has had the opportunity to test and train its consultants in ENISA's risk assessment and management methodology for SMEs, as well as to analyze the market for potential customers.

CEEI, as a public owned (Junta de Castilla y León) company who focuses on SMEs fostering and innovation, has offered to its base costumers (SMEs) the opportunity to introduce risk management process, being aligned in this way with similar activities encouraged by different local and national organisms such as for example INTECO's SGSI adequacy for Small Companies.

A.L.H.J Mañas S.L has contributed to this pilot as RM tool provider: Pilar Basic.

P.D. Jose Antonio Mañas is a prestigious professor in the Politechnical University in Madrid and has developed several Risk Management tools such as Chinchon, EAR or the standard PILAR tool that is aimed for Magerit Methodology.

A.L.H. J. Mañas S.L. has been able to adapt ENISA risk management modules for PILAR Basic RM/RA Tool, gaining insight and understanding regarding tool usability and performance and also analyzing applicability for new potential clients.

Finally, for the four SMEs participating in the pilot, they have had the opportunity to have implemented risk management process following a full-outsourcing scheme taken by GMV. They also have had the opportunity to be taught about Risk Management in general, good practices and Risk Management maintenance through the adapted tool PILAR

Selection of the SMEs and Micro Enterprises

The selection was made by GMV –Soluciones Globales e Internet S.A delegation in Boecillo with the support of CEEI.
The CEEI is the European Centre of Enterprises in the Castilla y Leon Area. It plays the role of facilitator for all the Small Companies that want to set up in this area. They are offered a place inside any of the CEEI buildings. They also get from CEEI some basical services as common reception and security guards or even a small canteen.

CEEI also promotes among its members support for innovation and growth. As this Pilot was regarded as an initiative in line with Security Awareness and Certification promoted by National Organisms, they collaborated by providing a grouped and vast number of companies with the desirable characteristics, among those of which the following ones were finally selected as they also show interest and can allocate resources in order to participate in the PILOT.

Category	Company Name	Activity
SME SME	**Instituto Biomar S.A.** http://www.institutobiomar.com/	Chemical and pharmaceutical industry
SME	**Machine Point, S.L.** http://machinepoint.com/	Industrial Machinery e-business
Micro-SME	**Próxima System** http://www.proximasystems.net	Industrial software
SME	**Besel S.A (Boecillo)** http://www.besel.es/	Technical Consulting

Category	Company Name	Activity
		Services on Renewable Energy

Table 1: SME selection

As it can be seen, those companies belong to different areas of interest, and make a reuse of IT technology but do not develop it by itself. So, for them, IT resources are a key point in achieving their business objectives though not the objective itself.

Instituto Biomar S.A is a company that is devoted to the discovery and development of new bioactive compounds from marine microorganisms.

Their development process starts with the collection of marine samples. Then, it is followed by the isolation of microorganisms from marine invertebrate and algae, and their analysis. Finally, they proceed to the study and identification of active secondary metabolites and further production of large amounts of them for commercial purposes.
They are also interested in forming productive collaborations with pharmaceutical, chemical, cosmetic and environmental companies to exploit its technology for product development and commercialization.
SoIT is an important tool for their development processes to ensure control and record of everything of interest.
Although their current Production Plant is located in Leon, inside Onzonilla's CEEI premise, they have plans to move in near future to a bigger laboratory.
So for them, it was an strategic goal to have done a Risk Assessment and further Business Continuity Plan, before moving.
Machine Point S.L is an international trading company specialized in selling second-hand machinery in the plastic sector.
They have contacts with more than fifty countries and their expertise lies in machinery for the film extrusion and converting; extrusion of pipes, tubes and profiles both rigid and flexible; PET performs, bottles, filling lines for soft drinks and water, disposable food packaging, packaging for the dairy industry, molded parts, compounding and thermoplastics recycling.
As they advertise their products or call for potential sellers in their Website and make e-Business, IT has become a critical point in their day-to-day business.

They are located in CEEI premises in Boecillo –Valladolid and have an own IT department compound of three qualified technical administrators.
Although they arrive to this Pilot by mistaking Risk Management with ISO 27001 certification, they admit being quite satisfied with the experience, as they have now reached an understanding of the Risk Analysis process and also of their own Business Processes that they do not have at the beginning. In addition, they have become the more proactive among the four studied companies in this Pilot and also showed their will to go on collaborating whenever is possible.

Proxima Systems S.L is specialized in industrial applications of Information Technologies.

There are mainly development solutions in the following areas:

- Remote monitoring and telecontrol of industrial processes, buildings, etc.
- Intelligent video surveillance over heterogeneous data networks.
- Industrial computing automation.
- Integration of hardware, networks and software in industrial and corporate environments.

This is the micro-SME studied and they are only nine people altogether. The average staff profile is a young but high-qualified engineer.

Besel S.A
Besel is a company specialized in the state-of-the-art for energy and environmental technologies.
Besel Consultancy solutions located in CEEI premises in Boecillo –Valladolid include:

- Technical and strategic consultancy.
- Process innovations and continuous improvement planning.
- Planning, management and development of projects.
- Training, awareness campaigns and publications.

On the following fields:

- Energy savings and efficiency
- Renewable energies
- Environment
- Mobility & Transport

For this company, IT is a key point in the SCADA processes. **SCADA** stands for Supervisory Control And Data Acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility based. In this case, it is related to infrastructure, which contains most remote terminals that send to a control point the information related to certain processes as for example, the water treatment. So Besel offers knowledge for setting these control points.

They rely much about IT technology, especially everything concerned with remote controlling, networking with remote terminals and therefore security is something they have in great concern.

Planning and Organization of work

During the deployment of the pilot, the following meetings were held:

- **Kick-off Meeting:** Held on the 14th July in GMV premises in Madrid.
    - Participants were ENISA, GMV and **A.L.H. J. Mañas S.L**

During this meeting, it was made some agreements over the overall procedure to be followed up and was formally accepted the proposal sent by GMV in response of the call for participants made by ENISA .

Basic aspects of the Pilot were discussed and scheduled such as:

- Preparatory Workshop preparation, dates, participants, materials, etc.
- Final Workshop rescheduled to mid November to have enough time for preparation and feedback from SMEs
- Customizing of Pilar Tool to be used with ENISA methodology approach.
- Regarded dates for intermediate progress reporting by GMV.
- Procedure with each SME for Risk Analysis development.
- Training for the GMV team on Pilar with ENISA methodology new library.
- Translation of documents of interest for the Pilot.
- ENISE II event articles in technical journals

- **Training Session on PILAR + ENISA library:** Held on 1st September in GMV premises in Madrid.
  - Participants were GMV Risk-Management team in the project and J.Mañas, who was the trainer.
  - Over the training some assumptions were made related to methodology approach for development the Risk Analysis on every SME. (See chapter **Error! Reference source not found.**).
  - GMV team asked J.Mañas to make further modifications to reflect better ENISA methodology. Modifications were scheduled for the following week as work with SMEs was to be in time.
- **Preliminary Workshop:** Held on 4th September in GMV premises in Boecillo.
  - Participants were GMV (Risk Team + Managers who have collaborated in SMEs selection), J. Mañas, CEEI, Machine Point (2 IT responsible), Proxima Systems (Manager).
  - Over this workshop, participants were presented to each other and GMV Risk Team explain the reasons and goals of the Pilot, how it was going to be carry out in terms of effort required to every participant, provisional dates for meetings, legal aspects to be bear in mind, deliverables, feedback required and possible dates for Final Workshop.
  - SMEs presented their business needs in terms of security. T
  - A basic introduction on Risk Cycle of life was presented by J.Mañas as we noted none of the SMEs have a clear idea on this matter.

- **Meetings with every SME:**

  - A devoted meeting was arranged with every SME, with an average duration of three hours – Four hours for the two companies who have not been able to attend the Preliminary meeting.
  - Meetings were in every SME premises including a tour of more or less twenty minutes to have evidence of basic aspects of Physical Security, Staff habits, and business development in a day-to-day basis.
  - The calendar for the Risk Analysis first interview was as follows:
    - **11th September: Machine Point S.L and Proxima Systems S.L**
      - We took advantage of the close location of both of these two companies to our GMV premises in Boecillo. So we managed to spend three hours with each one that day and afterwards the IT RM team had an internal meeting in GMV premises in Boecillo to discuss over information obtained.
      - In the case of Machine Point S.L we interviewed the IT department at a whole (3 members) + occasional questions to selected staff by the IT members when appropriate.
      - In the case of Proxima Systems S.L. (micro-SME) we interviewed the manager and Technical Developer responsible and also the IT administrator.
    - **16th September: Besel S.A.**
      - We devoted the whole afternoon to this company, making an introduction to the Pilot, Risk Management and Pilar Tool as they were unable to make the Preliminary Workshop.
      - We interviewed the IT manager and also for some technical issues, two consultants who were appointed by the IT Manager to answer some questions that arose in the middle of the Risk Analysis.
    - **23rd September: Biomar S.A**
      - We interviewed the Product Manager and some staff: Researcher in charge of main projects, and also some administrative personnel.
      - We also provided them an introduction to the Risk Analysis, the ENISA Pilot grounds and Pilar Tool.

After every Risk Analysis was made further doubts were answered by phone by designed point of contacts provided during the first interview.

E-mail was only used to arrange new meetings or any other issues not related to confidential information as NDA was signed by every party in the first meeting and procedures were clearly stated.

- **Report delivering and discussion with every SME:**

After reports were finalized and all doubts were clear, we arranged again meetings with every Point of Contact designed for this task that was also present in the meeting for carrying out the Risk Analysis.
During these final meetings, in addition to handled them in a confidential way, the deliverables we discussed with them the results, the recommendations and about all, we had again their feedback about the experience.
We also helped them to install Pilar Tool – As we also included in the deliverable package their license file provided by J.Mañas.
We also reviewed with them the file with their report in Pilar format and teach them on how to maintain that file updated for their Risk Analysis report.
Finally, we showed them how to obtain reports from the tool and what information was put on these reports so they can have a useful dossier for Board of Directors decisions supporting.
On average, we devoted one hour and a half on every interview.
The deliverable package consisted on a bounded report printed in color with their Risk Analysis Report and a CD containing the same report in pdf format, the installation file of Pilar Tool and their license file. We also included the final questionnaire in doc format so they can modify it and give it to us back easily.

  - Meetings scheduled:
    - 29th September: Machine Point S.L and Proxima S.L.
    - 6th October: Besel. S.A. Matrix premises in Madrid.
    - 8th October: Biomar. S.A. Manager's private Desk in Madrid.

Although it was said to SMEs to give back their answers in ten day's time, it took them up to the first week of November to send us their feedback. Some of them claimed that it tooked some time to become used to the Pilar Tool but some others were only because of lack of time for this task.
There was even a SME – Besel.S.A – Which was reluctant to give an answer and finally sent it to us after more than three weeks after we gave them the deliverable package.
It must to be mentioned that this company has many other locations in Spain and the Point of Contact they gave us – IT manager - was commuting from one location to other quite often, what was quite a nuisance for us because it delayed the feedback task collecting.

- **Meeting with J.Mañas to have his feedback over the Pilot:** 23rd October in Leon.

As we were invited by INTECO to participate on ENISE II event with our experience with SMEs and new ENISA approach - see references made and agenda in this website:
https://2enise.inteco.es/component/content/article/99-agenda-t32

So we met up the evening before the event premises to coordinate our presentations – and discuss over the Pilot experience with most of the feedback already provided by SMEs.

We also discussed on how to enhanced the tool and also ENISA approach to satisfy the requirements made by SMEs.
On the 24th, we made dissemination on the ENISA approach, how the procedure with SMEs has looked like and overall result so far. J.Mañas show how Risk Analysis for a SME could be easily carried out through PILAR tool with ENISA library provided.

- **Final Workshop:** Held on the 10th of November, in GMV premises in Boecillo.
  - Participants: ENISA, GMV, CEEI, J. Mañas and Machine Point S.L.

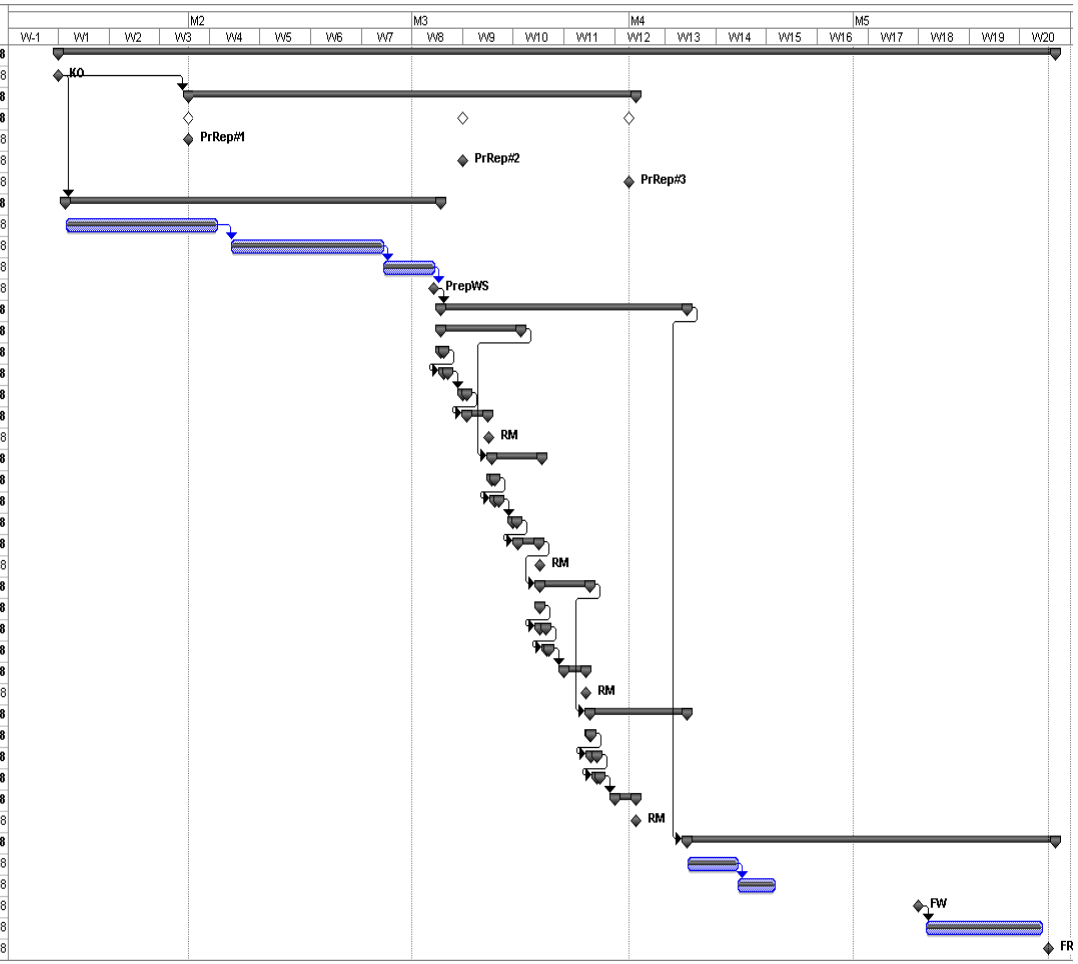
During this final meeting, GMV offered a presentation with basic results on the feedback made by companies, which were clarified by Machine Point S.L

whose IT department participated in quite a proactive way, providing explanations to some issues observed related mainly to lack of previous knowledge on Risk Analysis and also with feeling a bit insecure about handling Risk Analysis.

There were also positive comments about the improvements on their business processes and to the whole company provided by the methodology. They also admitted having worked before in a numbness way with reference to Risk handling although they express they have been always interested in Security.

Although Proxima Systems S.L could not participate in the project, they express their wish to go on participating in any other initiative promoted by ENISA and so did Biomar S.A.
Both Proxima Systems S.L. and Machine Point S.L. had requested GMV for information related with local initiatives in similar issues such as the INTECO SGSI project for SMEs.

ID	Nombre de tarea	Duration	Start	Finish
1	**ENISA Risk Management Implementation Pilot**	**100 days?**	**Mon 14/07/08**	**Fri 28/11/08**
2	**Kick-off Meeting**	1 day	Mon 14/07/08	Mon 14/07/08
3	**Activity 1 Project Management and Product Assurance**	**44 days**	**Fri 01/08/08**	**Wed 01/10/08**
4	**Progress Report Submission**	**44 days**	**Fri 01/08/08**	**Wed 01/10/08**
5	Progress Report Submission 1	1 day	Fri 01/08/08	Fri 01/08/08
6	Progress Report Submission 2	1 day	Mon 08/09/08	Mon 08/09/08
7	Progress Report Submission 3	1 day	Wed 01/10/08	Wed 01/10/08
8	**Activity 2 Preparatory Activities**	**38 days?**	**Tue 15/07/08**	**Thu 04/09/08**
9	ENISA Methodology - Document Translation	15 days	Tue 15/07/08	Mon 04/08/08
10	Training in PILAR & ENISA Methodology	15 days	Thu 07/08/08	Wed 27/08/08
11	Workshop Preparatory Activities (documentation, presentations, etc.)	5 days	Thu 28/08/08	Wed 03/09/08
12	Preparatory Workshop	1 day?	Thu 04/09/08	Thu 04/09/08
13	**Activity 3 Implementation of Risk Assessment Process**	**24 days**	**Fri 05/09/08**	**Wed 08/10/08**
14	**SME#1 Risk Assessment**	**7 days**	**Fri 05/09/08**	**Mon 15/09/08**
15	**Phase 1 - Risk profile selection**	**0,25 days**	**Fri 05/09/08**	**Fri 05/09/08**
18	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Fri 05/09/08**	**Fri 05/09/08**
22	**Phase 3 - Control Cards Selection**	**0,5 days**	**Mon 08/09/08**	**Mon 08/09/08**
26	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 08/09/08**	**Thu 11/09/08**
29	**Risk Management Report**	2,5 days	Thu 11/09/08	Mon 15/09/08
30	**SME#2 Risk Assessment**	**5 days**	**Fri 12/09/08**	**Thu 18/09/08**
31	**Phase 1 - Risk profile selection**	**0,25 days**	**Fri 12/09/08**	**Fri 12/09/08**
34	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Fri 12/09/08**	**Fri 12/09/08**
38	**Phase 3 - Control Cards Selection**	**0,5 days**	**Mon 15/09/08**	**Mon 15/09/08**
42	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 15/09/08**	**Thu 18/09/08**
45	**Risk Management Report**	0,5 days	Thu 18/09/08	Thu 18/09/08
46	**SME#3 Risk Assessment**	**5 days**	**Thu 18/09/08**	**Thu 25/09/08**
47	**Phase 1 - Risk profile selection**	**0,25 days**	**Thu 18/09/08**	**Thu 18/09/08**
50	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Thu 18/09/08**	**Fri 19/09/08**
54	**Phase 3 - Control Cards Selection**	**0,5 days**	**Fri 19/09/08**	**Fri 19/09/08**
58	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 22/09/08**	**Wed 24/09/08**
61	**Risk Management Report**	0,5 days	Thu 25/09/08	Thu 25/09/08
62	**SME#4 Risk Assessment**	**9,5 days**	**Thu 25/09/08**	**Wed 08/10/08**
63	**Phase 1 - Risk profile selection**	**0,25 days**	**Thu 25/09/08**	**Thu 25/09/08**
66	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Thu 25/09/08**	**Fri 26/09/08**
70	**Phase 3 - Control Cards Selection**	**0,5 days**	**Fri 26/09/08**	**Fri 26/09/08**
74	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 29/09/08**	**Wed 01/10/08**
77	**Risk Management Report**	5 days	Thu 02/10/08	Wed 08/10/08
78	**Activity 4 Risk Assessment Results**	**37 days**	**Thu 09/10/08**	**Fri 28/11/08**
79	Risk Process Results Analysis	5 days	Thu 09/10/08	Wed 15/10/08
80	Workshop Preparatory Activities (documentation, presentations, etc.)	3 days	Thu 16/10/08	Mon 20/10/08
81	**Final Workshop Celebration**	1 day	Mon 10/11/08	Mon 10/11/08
82	Final Report Preparation	12 days	Tue 11/11/08	Wed 26/11/08
83	**Final Report Submission**	1 day	Fri 28/11/08	Fri 28/11/08



2.C Methodology Deployment

GMV is a company with a large experience in Risk Assessment. Our approach to this Pilot was to consider only the outsourced option for carrying out the Risk Analysis in the four companies selected.
This decision was supported by the fact that none of that companies in the database provided by CEEI has been taught in Risk Analysis previously. In addition, they do not have enough human resources to achieve this task even in the case that GMV could give them enough training. However, they should compromise some resources and time for succeeding in this collaboration for the Pilot.
In addition, our experience using **PILAR tool** developed by **A.L.H. J. Mañas S.L** for Risk Analysis using Magerit Methodology, made us also think again on this tool to be adapted to the new methodology.
Before of all, and after being read of ENISA approach through the documentation provided by them, we try to synthesize it in a four-step procedure to be followed-up.
The first step was to determine the profile of the company according to financial, legal, production issues or staff conditions. We try to search about legal considerations that might apply to every company just by checking the area and services that every company was providing. This was done before having the first interview.
As for example, if we read about Machine Point in their website and we realized they contacted potential customers by Internet, then e-Business laws might apply to them or else Personal Data regulations as for example, Spanish laws LOPD or LSSI related to electronic personal data use or spam considerations as well as logs to be kept or any other issues such as privacy, integrity, mail use or so.
We also try to figure out the size of the company – if public information is provided – or if there has been any new posted and related to those companies, that might tell us about incidents, solvency problems or anything of interest.
With previous researched information, we developed both a preliminary questionnaire – See Annex and also a set of possible doubts or questions that might arise during the first interview with the company.
To guarantee privacy of the security vulnerabilities or features that GMV might learn from companies and as part of the code of ethic that GMV has, a **Non Disclosure Agreement** must be signed by both parties – Every SME or micro-SME and GMV – prior to have any non public information about every company.
As the answers to this questionnaire might be regarded as Confidential Data, questionnaires should be used by companies to determine who should be present in the first interview. They must provide information such as how many workers the company has or else how many days without the critical business process the company can stand without a dramatic lost.
When it comes to company profile, a default value meaning **no significant** was added as it was not regarded previously among possible selections. This value will apply when the aspect treated has nothing to do with the company, as for example, financial issues or legal issues, etc.

Once classified the company, there comes the second step in which four types of assets were chosen among all in order to have the most relevant features of the companies.

Time, resources and previous knowledge were factors to be sized before developing our strategic plan that will include at least one extended interview with board of directors or business managers capable of providing us the big picture of their business processes as well as the technical staff in charge of every single process or at least a number of them enough to determine whether certain safeguards have been set or not.
So, just with the large interview, our purpose was to draw a draft on the Risk Analysis that should be adjusted after an overall review and check to determine inconsistencies when answering the questions or any other consideration that might be leave out unnoticed.
On the other hand, apart from making questions related to safeguards mentioned in the corresponding cards, some aspects were reviewed on-site. For example, if we ask them whether they provide security awareness to employees and we notice some issues such as passwords written in post-it notes close to an employee's PC or they usually leave their PC without blocking or things like that, this safeguard is not successfully applied although they claim to. Same for physical security safeguards that can be reviewed easily as we pass through the premises.

3.C Methodology related issues.

Outsourcing Options

The three outsourcing options offered by the methodology are enough to include every possible situation and circumstances of any SME. Nevertheless, the three set of questions used to determine the right decision may be too repetitive and confusing. Probably, the best option, and the one chose by GMV in the methodology implementation, is to group every different question in one single questionnaire. This simplified questionnaire is the one that the SME should complete. Then, the number of positive answers could easily be mapped into the outsourcing options. The simplified questionnaire used by GMV in the implementation can be found in the first questionnaire of Annex I.

Risk Profile Selection

As an overall comment, to our understanding, ENISA **approach for determining the company profile does not take under consideration the three common measurements of the security**, that is : **Integrity, Confidentiality and Availability**. As for example, we can imagine a company that sells its products by Internet, but do not contain in its web any critical information that should not be disclosed. For this company, Availability and Integrity is of great interest but not Confidentiality. However the reverse case could be a company that develops cryptographic material for military purposes and stores particularities of the items developed in a database for accounting purposes with the name of the items, invoicing information, delivery details and the algorithm applied. For them, keeping safe the algorithm used to make the ciphers is critical but not so critical to have available the whole database in a 24x7 basis, however Integrity also must be a important although might be not so critical issue as a mistake in the disclose to end customer could lead to a unsuccessful attempt to communicate through the purchased cipher. However an enemy knowing the algorithm used in the cipher is the most critical issue related to the information.
Taking under consideration the three dimensions of security, would be of interest when selecting safeguards or either when making recommendations about what the target levels should be.

In addition, there are many aspects that could be included in the **risk profile identification questionnaire to obtain a more accurate result**. Most of the subjects dealt in the questionnaire are quite general and so it is no surprise that we obtained nearly the same risk profile for every SME.
In our opinion, **questions related with yearly revenues** could be interesting, but they **are not critical aspects,** especially when the decision limits are five and twenty-five millions and we are talking about SME's. A similar thing happens with Productivity risk area. Although this questionnaire has been used exactly as it's explained in the methodology, many other considerations could be include identifying the risk profile and selecting then the best safeguards.

Another consideration made that is included in Pilar Tool but not in ENISA approach is the **profile of the potential attacker**. Although not every risk is human made, at least it introduces concern about who could have an interest of attacking the company. For instance, in the military case, an enemy country, in the case of a innovative researcher, maybe an industrial competitor or else in any case a discouraged former employee. Motivation to attack is something we consider as of interest at least to encourage companies to make an exercise of self-reflection. Potential attacker will modify the type of threats we can expect and also the threats likelihood.

Such consideration has been included in Pilar tool under the menu "Domain modifiers". It consists in several aspects classified in different categories. Those aspects are taken under consideration when trying to identify the potential attacker profile. The attacker profile will modify the type of threats we can expect and also the threats likelihood. The attacker profile has been mapped in Pilar tool by a multiple selection list with the following options – English translation is provided aside in blue:

Identificación del atacante /Attacker profile
Público en general /General Public
Competidor comercial /Commercial competitor.
Proveedor de servicios /Service Provider.
Grupos de presión política /activistas /extremistas / Political Activists, extremists.
Periodistas /Journalists.
Criminales / terroristas / Criminals, terrorits .
Personal interno / Staff Members.
Bandas criminales /Gangs.
Grupos terroristas /Terrorits groups.
Servicios de inteligencia / Intelligence Services.

Table 2: Potential attacker

Motivación del atacante/Attacker Motivation
Económica /Financial.
Beneficios comerciales /Commercial Benefits.
Personal propio con problemas de conciencia/Staff members with a guilty conscience.
Personal propio con conflictos de intereses/Staff members with conflict of interests.
Personal propio con pertenencia a un grupo extremista/Staff members who belong to an extremist group.
Con ánimo destructivo /With aim of causing destruction.
Con ánimo de causar daño /With aim of causing damaging.
Con ánimo de provocar pérdidas /With aim of provoking financial losses.

Table 3: Attacker motivation

Beneficio del atacante/ Attacker Benefit
Moderadamente interesado /Milded interested
Muy interesado /Very interested

Extremadamente interesado /Extremely interested

Table 4: Attacker Benefit

Motivación del personal interno /Staff Members Motivation
Todo el personal está fuertemente motivado /All the Staff members are strongly motivated.
Baja calificación profesional / escasa formación//Low professional qualification, lack of enought training.
Sobrecarga de trabajo /Work overloaded.
Con problemas de conciencia / Conscience troubles.
Con conflictos de intereses /Conflict of interests.
Personal asociado a grupos extremistas/Staff members associated to extremists groups.

Table 5: Staff members motivation

Permisos de los usuarios/User Permissions
Se permite el acceso a Internet
Se permite la ejecución de programas sin autorización previa
Se permite la instalación de programas sin autorización previa
Se permite la conexión de dispositivos removibles

Table 6: User privileges

Conectividad del sistema de información/Connection to the Information System
Sistema aislado /Isolated System.
Conectado a un conjunto reducido y controlado de redes/Connected to a reduced number of Networks that are under control.
Conectado a un amplio colectivo de redes conocidas
Conectado a Internet

Table 7: Information systems connectivity

Ubicación del sistema de información
Dentro de una zona segura
En un área de acceso abierto
En un entorno hostil

Table 8: Information systems location

Most of the previous aspects provide very interesting information to suggest useful safeguards to the SME.

Asset Identification

When it comes to **Critical Asset selection and classification**, it has been difficult to identify the asset category of each critical asset identified, especially when the critical asset is considered as a suit of components, and each of those components is an asset with its own category. As an example we can think on a company which critical asset is an e-commerce application (application category) and whose components are a database, a firewall, a network segment and a server (most of them system category). Each of those components has its own category and probably will require

different safeguards depending on that category. Nevertheless, the methodology score card selection will be based only in the critical asset category and will not consider at all the components category. A similar thing happens with security requirements selections since each of the components will have situations different requirements and it should be reflected in the safeguards suggested. In addition, a data or information repository could be useful in some cases and could be easily mapped with access control safeguards, user privileges, etc.
So we introduced some new asset subtypes we have regarded as important such as for example **Printers, PBXs** – They make connections among the internal telephones of a private organization — and also connect them to the public switched telephone network (PSTN) via trunk lines, and therefore, we regarded as of interest in general, not only for this Pilot. This is also valid for **Firewalls**, as regarded also of interest to safekeeping the networks against intruders.

On contrast to ENISA approach, Pilar Tool allows **Asset information to be added,** we took advantage of this feature to add as much information as it was of interest, so also companies can make further use of this feature for inventory purposes or any other plans as for example Disaster Recovery or Asset Maintenance

Asset Category	Asset types
Systems	Printer
Network	Firewall PABX
Applications	Database Management system Office Web server Web client Email server Email client

Table 9: Additional asset types

Control Cards Selection

Most of the control cards selection considerations are related to the asset classification and have been already mentioned in previous section; nevertheless, another important aspect is threats and their influence. As **ENISA approach does not regard threats,** as Risk Management lifecycle usually do, but as so does Pilar Tool, we decided to select a subset of threats of interest per asset to be used within the Pilot – Not the whole Magerit v.2 set suggested but at least the most common ones. Here it is given the threats we regarded of interest per Asset Category:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración

[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Table 10: Threats for Applications

Equipos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Table 11: Threats for systems

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio

[A.25] Robo de equipos
[A.26] Ataque destructivo

Table 12: Threats for networks

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Table 13: Threats for people

However, we found that Pilar Tool does not take under consideration **modifiers for threats likelihood**. It is something we regarded as of high interest as not every company has the same probability of suffering the same problem.
Imagine for example that we pay attention to physical threats to a database server. It is not the same if the company is a laboratory that deals every day with flammable or chemical substances – as for example Biomar S.A than a company that is located in a controlled place and only manages current desk materials – as for example Machine Point S.L. So in the same way, the likelihood of fire damage as a threat to the asset regarded is not the same for both cases. In the first case, we should recommend higher fire protection measures and, in the second case, only standard measures.

Pilar tool also adds, plus to ENISA recommended, **additional safeguards**. Those safeguards were chosen from the suit provided by the methodology but not directly extracted from the score cards mapping. We also try to keep them as short as possible and, in order not to introduce confusion in the reports we provided them in a separate chapter, noting that this was additional safeguards recommended by the tool and not by ENISA. In addition and using our expertise, we also by means of the Executive chapter in the report, add some understandable recommendations so board of directors could easily read this summary and pay attention to these overall recommendations.

Report generation and risk map charting: Using Pilar Tool has also provided fully reports using a standard GMV pattern for reports. Reports, graphics and reporting tools are useful to give Board of Directors a quick and easy view of the Risk status, targeted levels, areas where lacks have been detected and points to improve.

As a consequence of every previous aspect, especially those explained in asset identification section, it is possible to identify specific safeguards that are not directly extracted from the score cards mapping but from the combination of GMV experience, attacker profile identification, critical asset subcomponents classification and specific SME security issues identification. In addition, those safeguards were chosen from the suit provided by the methodology as a next recommendable step on a continuous improvement cycle.

Implementation and Management/ Gap Analysis

Related to the methodology safeguards, we would like to notice that **some safeguards proposed are a bit too long to fully catch the meaning**. As a recommendation, **cutting them into smaller pieces and giving more examples of application could be of high value for SMEs**. We have had to make an effort to translate in practical some safeguards and only after we provided some examples they understood the meaning.
Pilar tool allows using degrees of setting of safeguards, which is extremely useful in order to simplify the gap analysis understanding. We have evaluated the maturity level for each control in five levels plus the **Non Applicable** one, where the safeguard regarded does not have to do with the company. We have done a gap analysis considering de current situation based on the meeting held with SME against the target situation based on GMV experience. The levels used to identify the maturity of each control are the followings:

- L0. Non Existent → That means that the safeguard is not even regarded, nor set
- L1. initial /ad hoc → The safeguard is not set, but is regarded, planned or partially set
- L2. Reproducible but intuitive. → The safeguard is set but not under a clear procedure
- L3. Defined procedure → The safeguard has been set and there is a clear procedure, with documentation
- L4. Managed and measured → The safeguard is set, has a clear and documented procedure and its presence and efficacy is measured and controlled.
- L5. Optimized → All the points in L4 plus optimized, that means that after measuring and control it has been improved to its maximum efficiency.

4.C GMS's General Comments and Observations

At this point, some general comments and observations are made, based on the RM Pilot experience.
Although every company was previously contacted before to be selected in order to know about the Pilot and the objectives of it, companies have **little or even mistaken idea about the Risk Management concept**. Moreover, **none of them have read about ENISA** or any related international institution They have only known about local initiatives such as INTECO or general in Spain such as "Asociación de Internautas" They are not subscribed to CERTS, they do **not pay attention to any specialized web and only few ones knew of Security issues by newspapers**, magazines or general purposed internet sites. So although they have heard of anti-virus, Trojans, malware, phishing or concepts related, they have **only end-user knowledge**, not appropriate for getting into business no matter the smaller their company is.

There is a **sense of non-alignment between Board of Directors and IT departments** or administrators in terms of security initiatives. It seems as **Board of Directors takes security mainly in terms of company public image,** seeking certificates to take commercial advantage from competitors. But for IT administrators there is a real concern about security, but as they do not have the overall business picture, they might pay attention to minor issues, mostly related to technical related incidents – virus, intruders, failures – rather than those that might well compromise seriously the Business Continuity – legal or organizational issues, as for example.
Most staff interviewed admitted that, they would like to implement recommended changes but there is a general lack of resources to achieve those changes if they are not regarded as critical by managers.

As security is a non-visible subject when everything works well, **prevention is not regarded as a priority**.
This is not only related to security but as overall problem in companies, there is an overall lack of interest in preventive measures. However and thanks to current Spanish regulations, most of Physical safeguards were set into place, mostly related to fire prevention. Same as for staff care and health conditions.
As the four companies were located in CEEI premises, physical access or overall physical security were similar managed in all companies. Depending on own procedures, some companies added additional measures but as overall, the maturity level of this safeguard was quite dependable of the CEEI buildings characteristics. In this way, CEEI or any type of global housing of new companies should also provide a Physical Risk Analysis to every company willing to be hosted as a preventive measure. We noticed that, as overall, information about the site and private guards were available in the two buildings studied.

None of the companies had documented all the procedures required. As documentation takes time, there is a general lack of it in SMEs studied. Staff that

should be in charge of this task are normally postponing it as it is not enough regarded of interest by managers.
Another interesting point is related to **Organizational Issues and policies,** with special regard to employees.
All the companies studied trust so much in their employees, as most of them have been in the company for long-term basis.
There is little control on the staff behavior and it is not so odd that users configure and take self-care of their own PC.
There is also a general lack of accounting or track of staff actions in servers or any other critical asset. It is also not so odd to **trust all the security of the company in only one person** as **no manager interviewed thought about the betrayal possibility.**

Another interesting point is Risk Management. Some companies do not play well their cards in this area.
When there is a risk, **they do not make a serious exercise of overweighting all the possibilities and the balance cost-benefit of the safeguard to be introduced**.
The appliance solution is always the best regarded and sometimes the only one considered.
Few took into consideration the Risk Transference option such as for example, Insurance although this is quite on fashion in Western Society culture of making business.

About our experience with companies, we found them – with the exception of Machine Point - not as proactive as we expected, though all the four devoted the time agreed with them previously. Number of IT administrators is critical in achieving in a proactive way Risk Analysis. It there is not a minimum number, Risk Analysis will be leaved out or not fully maintain through years.

The best **lesson learned** by all the companies is that **Risk Analysis** is a **DUTY** before promoting any initiative or investment in security. They also have learned to identify their goals, priorities, business processes and critical assets. Finally, they have been taught into continuously Risk Analysis, by either on a time basis or at least every time their business needs or goals change or there is a modification in the critical assets inventory.

All the company reported that thanks to this Pilot they have noted **risks never regarded before**, as for example, those related to lack of Separation of Duties, lack of documentation or any other related to best security practices in an Organization.

5.C General findings

The risk Management methodology for SMEs is a simplification that allows the small and medium Enterprise discovering the general security situation in their organization easily and intuitively. Moreover, the methodology allows identifying which actions should be taken to efficiently improve the security situation.

The main negative aspect detected is that there is a sense of non-alignment between Board of Directors and IT departments in terms of security initiatives. Most staff interviewed admitted that they would like to implement recommended changes but there is a general lack of resources to achieve those changes if they are not regarded as critical by managers. It seems as Board of Directors takes security mainly in terms of company public image, and they don't pay attention to other issues that might compromise seriously the Business Continuity.

In addition, the SMEs general thinking about the risk profile identification questionnaire is that questions are extremely general and they don't provide enough information about the specific threats and risk of the organization.

So, generally speaking, IT administrators thought that it would help introducing information about potential threats and what-if scenarios together with likelihood measures in order to raise awareness among management.

When it comes to the subject of dealing with safeguards determination, we would like to notice that most of the SMEs have found some problems mapping the suggested safeguards with practical implementations and they demanded us information on costless solutions to implement safeguards regarded by ENISA methodology. To our understanding, more practical explanations would be a great help for them in order to implement the safeguards.

By the way, the gap analysis process is an important but complicated step for the SMEs, to suggest a target implantation level for the safeguards could be a good approach to make it easier. The five level approach used in the report to identify the present and target implementation level for safeguards has been proved to be easy and understandable enough in order to allow the SMEs doing it by themselves.

Nevertheless, every SME participating in the pilot think that ENISA approach is good enough for them and it has motivated them to apply the risk management process in their day-to-day work. Moreover, most of the SMEs participating in the pilot admit to have increased their knowledge in themselves, especially about their critical assets, its security requirements and what they can do to protect those assets.

6.C Feedback from companies

To facilitate companies the feedback report through the Pilot, as well as a final interview at the time of report presentation with comments from personnel designed, a questionnaire was issued to companies with time enough to answer after the report was read.
Companies can test and experience with Pilar Tool its own report in the format used by the tool which was also issued to them inside a CD together with the temporal license as agreed in the Preliminary Workshop.

Here it is provided the average from companies and translated into English

Answers range from 1 – Nothing at all to 5 – Satisfactory

REPORT EVALUATION	**4**
Is the report generated easy to read and to understand?	3,75
Is the report comprehensive enough?	4
Does the report Provides new information about risk management and assessment?	3,5
Do you think the recommended controls and countermeasures are suitable?	4
Are you going to implement at least one of the recommended controls in the future?	4
GMV INTERVIEW EVALUATION	**4**
Do you think it has been easy to deal with GMV?	4,25
Has GMV been able to understand the security requirements of your company?	4
Has GMV provided to your company a new point of view about security?	3,75
Has GMV provided to your company “new knowledge” about risk management and assessment?	4,25
Do you consider that GMV has spent enough time?	4
WORKSHOP EVALUATION	**4**
Was the meeting arranged with sufficient prior notice?	4
Were the contents of the presentations of your interest?	3,5
Do you consider the time spent in the Workshop has been enough?	4
Has the Workshop showed the most important objectives of the project?	5
Has the Workshop satisfied your expectations?	3
ENISA RISK ASSESSMENT APPROACH EVALUATION	**3,75**
Is the ENISA risk assessment approach clearly defined in the report generated?	3,33
Do you think that such approach consider the most relevant aspects of your organization?	4,75
Would you like to know more about risk assessment or the ENISA approach?	3,33

Is your organization more motivated now than before your participation in this Project to make progress in security information management aspects?	4,33
Do you feel comfortable with ENISA risk assessment approach?	3,33
PILAR SOFTWARE EVALUATION	**3**
Do you think PILAR is useful in the risk assessment process?	3
Do you think PILAR is easy to use?	2,5
Do you find useful the kind of reports generated by PILAR?	3
Do you understand every risk assessment concept used by PILAR?	3,5
Are you going to use PILAR in the future?	3,75

As a result of this questionnaire and with comments made by the final interview and the Final Workshop there come some conclusions:

1.- **Report generated with the Risk Analysis per company and time devoted by GMV to every company is very good in general**, although we feel we could have extend a little bit more about Risk Analysis and Risk Management process in overall, as it is the start point to understand any methodology suggested. Another point of interest is the language used. Though we have added an executive summary readable for the Board of Directors, we have the sense that they wanted more graphics, and more "**what if"** scenarios to give Board of Directors ideas on the consequences of the incidents that might arise because of the threats due to lack of safeguards.

2.- **Preliminary Workshop and Final Workshop,** although they were quite interesting for those companies present, they have not reach enough quorum because more than half of the companies did not attend despite they were recall with time enough.

3.- **ENISA approach is good enough for companies**, however some clarifications, improvements and introduction will be highly desirable for companies to understand what is all about.

4.- **PILAR basic Tool used for Risk Management and Report generation is also good enough for companies**, however it must be improved to facilitate SMEs a better installation and use. Most of the users in SMEs that are likely to go on using this tool admit they will not be capable of making a new report from scratch but only to maintain the file provided by GMV.

5.- **PILAR tool succeeds in terms of Risk Management understanding**. It contains a very nice help menu that explains fairly well every concept related to Risk Management.

7.C References

Below it is referenced the documents and references that have been used to deal with the new ENISA Risk Assessment Methodology within this PILOT.

Code	Name of the Document
[ENISA-INF]	Information Package for SMEs
[ENISA-RM&IT]	Risk Management & IT Security for Micro and Small Businesses
[ENISA-WWW]	*http://www.enisa.europa.eu*
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[BIOM-WWW]	*http://www.institutobiomar.com*
[MACH-WWW]	*http://machinepoint.com*
[PROX-WWW]	*http://www.proximasystems.net*
[BESEL-WWW]	*http://www.besel.es*
[ASINT-WWW]	*http://www.internautas.org*