FAQ to the report on "Assessing a simplified Information Security approach"

Why has ENISA conducted this report?
This report evaluates the feedback from the organizations involved in a pilot around a simplified approach to risk assessment and some aspects of risk management delivered by ENISA in the "Information Package for SMEs".

Why did ENISA come up with the "Information Package for SMEs"?
With the objective to stress the fundamental role of risk assessment and management in the protection of IT-infrastructure, ENISA's efforts to create awareness in SMEs and Micro Enterprises (MEs) started in 2007. This has been achieved with the ENISA deliverable "Information Package for SMEs", which is the first of ENISA's attempts to address the issue of Risk Assessment and to some extent Risk Management (*ENISA simplified RA/RM approach)*. One of the main reasons for the simplified version is the idea that SMEs need simple, flexible, efficient and cost-effective security solutions and guide non-expert users in the complexity of RA/RM activities.

Could you describe the approach and the purpose of it?
The approach is a one-size-fits-all solution created for non-expert users and for small organizations with relatively simple IT-components.
In the simplified RA/RM approach, 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.

What were the main objectives with the project?
The main objectives of the project were to:

- Assess the level of awareness on RA/RM in SMEs of various types and try to raise awareness by introducing the ENISA simplified approach in these SMEs.

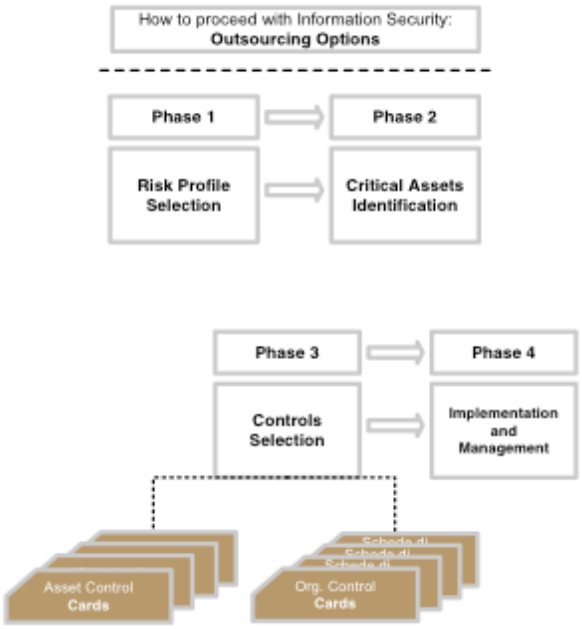
- Evaluate the applicability of the simplified RA/RM approach for SMEs in "real world" situations and
- Get feedback from the pilots in order to improve the approach and increase the potential value for SMEs.

Who participated and how did you evaluate the approach?
Three multiplier organizations were selected for the Pilot, each bringing in some representative SMEs/MEs from their areas/sectors. The selected multiplier organizations were GMV Soluciones Globales Internet (Spain), IAAITC (UK) and University of Bologna (Italy).

More than 10 pilots were performed to check the applicability of the simplified RA/RM approach and the results are presented in this report. The particular reports submitted by the pilots are also available as additional material to this report.

What are the components or the simplified RA/RM approach and what where the identified issues raised from the pilots?
All the comments raised from the pilots are grouped according to the components of the simplified RA/RM approach. The components of the approach are:

- Outsourcing options
- Risk profile selection (Legal and Regulatory impact, Productivity impact, Financial stability impact and Reputation and loss of customer confidence)
- Critical Asset Identification
- Control Cards Selection
- Implementation and Management (Gap Analysis and Mitigation Plan)



For each component part of the approach that received comments from the involved organizations ENISA provided its own considerations.

What are the conclusions?

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

- The approach received a generally high level of appreciation from the SMEs and MEs involved in the pilot.
- The approach led to an increased level of awareness on the fundamental role of Information Security RA/RM. 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 companies.
- The multipliers agreed on the need to introduce some customizations to the ENISA approach.
- 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 inevitable.

What else does the pilot result in for ENISA?

Apart from the challenges faced in the performance of the pilots with very small businesses, the results are rather encouraging especially as far as the impact of the Information Package for SMEs is concerning. 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 and need to be encouraged to focus on other priorities, they need to be supported with the right tools.

Did the cooperation with the multipliers work out the way you hoped?

ENISA's strategy to give the 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.

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

What will ENISA do to further improve the Information Package for SMEs?
ENISA will put in place a medium term plan to improve the Information Package. From comments, suggestions and ideas raised from the organizations involved in the pilots, ENISA has identified areas for future development of the simplified approach. These changes are both in terms of the structure of the approach as well as in terms of content and in the short term the Agency will focus mainly on revisions of the content.

What are some of the improvements ENISA will make?

- The Risk Profile Selection Phase will be reviewed to make the task clearer and more straightforward.
- The results will better address the need of small and medium enterprises.
- Some more structural changes will be applied in the short/medium term.
- From the structural point of view, two main adjustments are under evaluation.

What will ENISA do to further raise the awareness among SME's?
Within the ENISA Work Program but also by means of other activities, the issue of SME-Security is going to be elaborated further. Some of the actions that ENISA will put in place in the next future are in the context of "Building Information Confidence with Micro Enterprises".

This effort will lead to the second version of the Information Package for SMEs, to the development and release of a simplified approach for Business Continuity Management for SMEs, as well as to the "Development of Security Toolkit for Intermediaries and Multipliers"

For the development of the Security Toolkit ENISA will provide an incentive to establish a platform bringing together relevant organizations from different Member States with the aim to increase knowledge and information on how to build capacity among their constituency. Thus ENISA will support the establishment of concrete peer-to-peer learning practices in the area.

19/02/09

www.enisa.europa.eu

The full report is available at:
http://enisa.europa.eu/doc/pdf/deliverables/sme_rarm_pilot.pdf

The press release is available at:
http://enisa.europa.eu/pages/02_01_press_2009_02_19_sme_rarm_pilot.html

For further details contact:
Daniele Catteddu, Risk Management Expert, RiskMngt@enisa.europa.eu
Ulf Bergstrom, Press & Communications Officer ENISA, press@enisa.europa.eu
Mobile: +30 6948 460143