Risk Management at ENISA

A road map - from objectives to achieve practical results

Dr. Louis MARINOS
Senior Expert in Risk Management, ENISA
Technical Department
firstname.LASTNAME@enisa.eu.int
Tel: +30 2810 39 1359
Fax: +30 2818 39 1895

P.O. Box 1309
71001, Crete, Greece

Risk Management at ENISA: a road map - from objectives to practical results

Executive Summary

In this report we analyze the strategic objectives formulated in the Regulation for the establishment of ENISA and we focus on:

- The actions required for the **development of best practices**;
- The actions for the **promotion of interoperable** Risk Assessment and Risk Management solutions and
- On various individual aspects to be encountered during the coming years of operation in the areas of Risk Assessment and Risk Management to achieve practical results.

Some further highlights of this document are:

- The **establishment of a Working Group** on technical and policy aspects of Risk Assessment and Risk Management;
- The generation of **inventory** for methods, tools and best practices and the establishment of a basis for the **comparison**;
- The generation of **overviews for existing policies and policy approaches** on risk management;
- **Road map** for the issue of emerging risks for the future work of ENISA, together with an initial collection of emerging risks and potential measurements to mitigate them;
- Finally, by establishing **contacts with ENISA stakeholders**, target group oriented requests and priorities are integrated in the abovementioned activities.

The contents of the ENISA Regulation

Risk Management is one of the major tasks of ENISA. The “promotion and development of best practices for risk assessment and for interoperable risk management solutions” is one of the main objectives formulated in the Regulation for the establishment of ENISA (art. 3 a), d), h) and i) of Regulation (EC) No 460/2004 of the European parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency). This statement underpins the role of Risk Management, both in terms of strategic objectives of the agency as well as an important activity in the information security domain.

Looking more closely into this objective two main terms can be identified: (a) *best practices for risk assessment* and (b) *interoperable risk management solutions*. In fact, these two terms have been placed under the scrutiny of expert on information security and IT operations. While a need for practical methods for Risk Management and Risk Assessment does exist, especially small organizations enterprises with limited access to resources and investment need to benefit the most and hence given priority in terms of deliverables. Such methods and tools are applicable up to the working level of network, application and information management.

In the remainder of this paper we take a closer look at the contents of the Risk Management and Risk Assessment objectives of ENISA and we analyze their role and possible implementations in the coming years.

Best practices for Risk Assessment

Risk Assessment stands for the central process aiming at the technical and scientific identification, classification and mitigation of IT risks via the deployment of measures for the protection of IT-assets at risks (i.e. the .valuable assets of an organization). Various security standards and methodologies available, introduce such processes to cope with the quantification of the risk potential to which assets are exposed. At the same time, through the use of measurements and controls (also referred to as security measurements and security controls) these standards provide the tools for the establishment of the required assets protection.

As Risk Assessment standards and methodologies are at a different level of abstraction, their use is subject to individual adaptations. Extrapolating Risk Assessment standards down to the working level for various forms of organizations is considered as best practices in this area.

Inventory of available standards

By making an **inventory of available standards**, **methodologies, best practices and tools,** ENISA currently conducts the first step towards the identification of existing approaches to Risk Assessment. For this purpose a Working Group on Risk Management

/ Risk Assessment has been established. Depending on the background of the Working Group members, an initial set of standards and best practices will be identified.

It is currently expected that this inventory will not be necessarily exhaustive of the situation on the ground. There might be national and industry standards and best practices, that will not be described in detail or even included in the current version of the inventory. A systematic approach for the inclusion (and eventually removal) of standards, methods, best practices and tools from the ENISA inventory will be introduced to allow stakeholders register emerging methods in Risk Assessment and Risk Management that are in use in their organizations.

Interoperability of Risk Management solutions

According to ENISA regulation, Risk Management is the process of weighting policy alternatives by selecting appropriate prevention and control options. This definition describes a variety of Risk Management solution, e.g. in the areas of corporate governance, information technology, critical infrastructure protection, environment, project management, etc.

Although this definition is applicable to all kinds of Risk Management standards, their contents, structure and delivered results vary significantly. When applied in combinations, Risk Management solutions with different content cannot interoperate. In the area of corporate governance, for example, there are no codes or guides on how information risks can be managed within the corporate governance framework. To this extend, information risks are not easily measurable at the level of executives.

Within the area of information Risk Management interoperability of various solutions has never been studied in detail. The results of various Risk Management solutions in the area of information technology are not directly comparable. Therefore, risk assessment results based on ISO 17799, for example, cannot be directly associated to those produced by using another Risk Management solution (e.g. German Baseline Protection Manual). Undesired effects might therefore come to life, if organizations using different Risk Management solutions seek to cooperate with each other. Assuming that organizations with different Risk Management solutions communicate in the context of an e-commerce application, the Risk Management practice related to this interaction cannot necessarily be directly identified, as the ground for the comparison of the particular solutions does not exist.

Paving the way to future Risk Assessment and Risk Management

While ENISA is in the phase of establishing operations, work on Risk Management and Risk Assessment is currently conducted within an ad hoc **Working Group on Risk Management**, a team consisting of nine experts in this area. The main focus of the ENISA Work Program of this year is the generation of an **inventory of Risk Management and Risk Assessment methods** currently in use, both at a Member State level as well as internationally. In addition, the Working Group has the mission to generate information packages for types of organizations to help them in selecting and applying suitable methods for performing and managing information security related risks.

The results of the Working Group are providing ENISA with one source of knowledge. By means of parallel activities in the middle terms, additional knowledge on Risk Management and Risk Assessment will be obtained. This will include:

- Establishing a “common language” to facilitate the communication between stakeholders in exchanging information about the methodologies and best practices used. This activity is the first step towards preparing interoperability of the methods;

- Establishing a dedicated technical infrastructure to gain hands-on experience by installing contemporary Risk Assessment and Risk Management methods and tools. The installed functions can be used for demonstration purposes (e.g. to interested stakeholders);

- Identifying the scope of Risk Management and Risk Assessment within the process of Security Management and other operational IT-processes;

- Comparing of Risk Management structures (e.g. audit based vs. risk collection approaches);

- Preparing a process to adopt additional methodologies, best practices and tools into the established inventory;

- Establishing a basis to raise awareness in the area of Risk Management and Risk Assessment;

- Facilitating cooperation among various European initiatives in the area of Risk Management that contribute to reach a common level of security;

- Generating a plan to address issues in the area of emerging risks in converging networks. To this extend, the anticipation of pro-active measurements for the identification of new threats and their impacts to networks will be accounted for;

- Integrating relevant results from current projects funded by the European Commission in the area of risk preparedness in European businesses.

At a later stage, the attention of the Work Group will shift to results emerging from relevant R&D activities at Member State and European levels, like:

- Algorithms for the identification of interdependencies between IT - assets (e.g. dependability). Particularly important is the representation of dynamic dependencies between the assets;

- Measurements for the quantification of risks (impact analysis, incident response);

- Rating infrastructure failure effects and risks;

- Generation of knowledge bases on existing threats and vulnerabilities;

- Pro-active Risk Analysis and Management (i.e. identifying risks before occurrence);

- Contribute to linking liability requirements and risk management requirements on a per application basis;

- Contribute to turning policies to a valuable instrument for the regulation of the risk posture of an organization;

- Active recognition of risk potentials (identifying risks after the occurrence of an incident, i.e. by analyzing new incidents and emerging vulnerabilities).

The Work Groups will additionally take into consideration emerging regulatory and legal requirements with regard to the content and format of security risks within a business environment. Moreover, by establishing contacts with the ENISA stakeholders, target group oriented requests and priorities will be introduced to the above mentioned items. Through the work of the coming years, ENISA will turn all these requests to useful contributions and effective support in the area of Risk Management and Risk Assessment.

./. November, 2005.