ENISA ad hoc working group on risk assessment and risk management

Road map

Deliverable 3

Final version

Version 1.0

30/03/2006

1. Preamble

In 2005 ENISA (European Network and Information Security Agency) set up an ad hoc Working Group on "Technical and Policy Aspects of Risk Assessment and Risk Management".

Experts from eight Member States cooperated through regular meetings within eight months. Based on "Terms of Reference", the objectives of the WG were to:

1. Produce an overview of existing RA/RM methodologies and the relevant players in this field, and comparison of the different methodologies.

2. Compose information packages for 2-3 types of organisations to help them in selecting and applying a suitable method for performing and managing information security related risks.

3. Propose a roadmap document.

To meet these objectives, the WG produced three documents: this document represents the results on objective three.

Content

2. Introduction

After discussions with both internal and external experts, the Risk Assessment / Risk Management Working Group (WG) identified the following areas worth being developed in the future.

For each identified area, the WG suggests a driver to help the reader better understand the identified need for a possible solution. Then, WG suggests a priority order for these areas by means of term to be addressed (short or middle term).

Some of the detailed points of each area have been formulated as questions in order to underline the related problems.

3. Identified areas

3.1. Area 1: Interoperability/compatibility of methods

Two different independent systems have been assessed with the same method. What happens, if the systems are then connected? (Solution: consider common sets of assets, threats and vulnerabilities, and risks generated by their interconnection).

Two different independent systems have been assessed with two different methods. What happens if the systems are then connected? (Solution: consider common sets of threats and vulnerabilities, propose some method for the evaluation of asset values and risks generated by their interconnection).

Two different methods cover different issues of risk management (e.g. corporate governance and IT security). How can these methods be connected?

Driver: Assessing information systems and combining them is becoming more and more common practice. In order to reuse existing results, some work on interoperability and compatibility is necessary. This area has already been identified (but not yet solved) by experts in the relevant field (e.g. EBIOS club).

3.2. Area 2: Comparability/merging of methods

One organisation needs to combine existing methods to achieve better results for their purpose (e.g. BSI.DE and ISO/IEC IS 17799). What are the meaningful combinations of (modules of) existing methods and how can different methods be optimally combined?

Driver: ENISA-BSI Information Security Management Workshop in November 2005 concluded that this issue is becoming more and more relevant.

3.3. Area 3: Method inventory maintenance

What are the functions needed to maintain an inventory? (Enter, remove or update methods and tools).

What is the sufficient amount of information needed to describe a method and how can this information be assessed? Who defines it?

What kind of quality assurance is needed to the inputs for the above points?

Driver: New methods / tools are constantly being developed. Existing ones are constantly maintained. This information has to be added to the inventory (e.g. at least one method has already been submitted to ENISA by the Italian member of PSG).

3.4. Area 4: Measurements of risks

Which (types of) qualitative methods do exist?
Which (types of) quantitative methods do exist?
Do any bridges exist between qualitative and quantitative methods? (This issue should also be addressed in area 1 (interoperability)).

Is it possible to improve existing methods based on knowledge from other fields (e.g. banking, insurance, critical infrastructures, aerospace)?

Driver: Comparability / compatibility / interoperability of methods require comparability / compatibility / interoperability of measurements of risks.

3.5. Area 5: Unified information bases for risk management

Information bases including the following points should be provided:

- Common definitions of threats
- Common definitions of vulnerabilities
- Common definitions of asset groups (e.g. good default definitions and values)
- Common representation schemes for risks or classes of risks

Driver: This is an indispensable condition to achieve comparability / interoperability / compatibility.

3.6. Area 6: Risk management and relevant security issues

The interfaces of risk management to other relevant security processes have to be identified, including:

- Risk management and product evaluations (e.g. Common Criteria)
- Risk management and Information Security Management Systems
- Risk management and security controls deployment
- Risk management and incident handling
- Risk management and Business Continuity Planning

Driver: A clear relationship to other areas is vital for the communication of risks to the relevant partners (e.g. experts, stakeholders, member states etc.).

3.7. Area 7: Business Continuity Planning (BCP)

Are there any European methods on BCP (which)?
Are there any standards on BCP (which)?
Are there any tools on BCP (which)?
Are there any good escalation schemes in BCP?

Driver: Business Continuity Planning is an integral part of risk management when facing continuity risks.

3.8. Area 8: Emerging risks

Are there existing models to identify emerging risks (which)?
What are possible threat agents (current and future)?
Are there any models to specify dependability (assets, threats, and attack scenarios)?
Are there any suggestions to gather and disseminate information regarding emerging risks?

Driver: Emerging risks is an important part for the enhancement of risk preparedness, as identified in ENISA regulation article 13.

3.9. Area 9: Awareness, training, communication

What is the content of professional material for dissemination and promotion of risk management?
What kind of methods can be used for dissemination purposes?
Are any demonstration programs necessary for training purposes?
What are the contents of such demonstration programs?

Driver: In many cases, lack of awareness has been identified as one of the most important vulnerabilities within IT security.

3.10. Area 10: Security measurement

What are the well-suited measurements of IT security (e.g. maturity level)?
How to estimate the coverage of risks by security measures?
How can IT security robustness be measured?

Driver: It is of central importance for managers to get comprehensive information on the security status of their IT systems.

4. Priorities on areas

4.1. Areas of short term priority (within the next 1-2 years)

The following areas seem to be of first priority, as they are a relevant follow-up to the deliverables already done by the WG and to the planned ENISA deliverables for 2006:

Area 5 is a prerequisite to fulfil the areas 1, 2 and 3.

Area 1 will improve the quality of description of each method by adding attributes related to interoperability issues between methods.

Area 2 will implement emerging requirements expressed by industrials and users.

Area 3 will increase exhaustiveness of method inventory and make it comprehensive and self-contained.

Area 7 is an urgent question because threats pervade geographical borders and BCP is a condition for risk management (cf. Project on preparedness for risk management and business continuity performed by INFSO on behalf of ENISA).

Area 8 is an issue to be addressed by ENISA (cf. ENISA regulation article 13).

Area 9 is an ongoing effort towards culture of security in Europe (See ENISA regulation article 14).

4.2. Areas of medium term priority (2-3 years)

Continuation of previous ones (5, 3, 1, 2, 7, 8, 9)

Initialisation of Area 4, Area 6, Area 10.

5. Areas suggested for a possible appointment of a WG

In order for users to successfully apply Risk Management/Risk Assessment methods, additional information about potential threats and vulnerabilities of assets is necessary. A future WG could propose a **database of threats, threat agents and vulnerabilities**. For this task, existing databases will be identified and put together to the appropriate context so as to conform to the inventory produced within the 2005 ad hoc WG on Risk Management (e.g. attributes, description method, connection to inventory of methods etc.).

Due to the structure and mandate of the Working Group, the delivered inventory is not exhaustive. In a new WG on Risk Management, **a submission process of new methods or tools and an updating process for existing ones** will be proposed. This will include the necessary quality assurance steps (e.g., reviews) to ensure consistency of the submitted information with the existing inventory.