Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

(Parts of this report constitute the deliverable defined in the ENISA Work Programme 2006 as:

"*Survey of existing Risk Management and Risk Assessment Methods*")

Conducted by the
Technical Department of ENISA
Section Risk Management

June 2006

Executive Summary

This report is the first ENISA deliverable 2006 in the area of Risk Management / Risk Assessment. Parts of this report constitute the deliverable defined in the ENISA Work Programme 2006 as: "Survey of existing Risk Management and Risk Assessment Methods".

The purpose of this document is to address identified open problems in the area of Risk Management and to provide a road-map for addressing further open issues at a European level.

This document contributes to solving the following problems:

1. low awareness of Risk Management activities within public and private sector organizations;
2. absence of a "common language" in the area of Risk Management to facilitate communication among stakeholders;
3. lack of surveys on existing methods, tools and good practices.

Further identified open issues/needs in the area of Risk Management / Risk Assessment, such as interoperability of methods and integration with corporate governance, are presented by means of a road-map describing and prioritizing possible future actions to be performed in that area.

Elements of work conducted within the ENISA *ad hoc Working Group on technical and policy issues of Risk Assessment and Risk Management* have been integrated into this document.

Contact details: ENISA Technical Department, Section Risk Management, Dr. L. Marinos, Senior Expert Risk Management, Jani Arnell, Expert Risk Management, e-mail: RiskMngt@enisa.europa.eu

Table of Contents

Table of Figures

1 Introduction

Risk Management, in general, is a process aimed at an efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses. It is an integral part of management practice and an essential element of good corporate governance. Risk Management should be an endlessly recurring process consisting of phases which, when properly implemented, enable continuous improvement in decision-making and performance improvement.

Information Security (IS) Risk Management can be a part of an organization's wider Risk Management process or can be carried out separately. Given that Information Technology in general (and Information Security in particular), incorporates state of the art technology that is continuously changing and expanding, it is recommended that IS Risk Management be established as a permanent process[1] within the organization.

Both within the documented ENISA tasks (s. ENISA regulation [ENISA Regulation]) and various events in the area of Risk Management, several problem areas have been identified that are worth addressing at a European level:

1. *Low awareness of Risk Management activities within public and private sector organizations*: The issue here is that those organizations implementing Risk Management often tend to neglect Risk Assessment. Other organizations rudimentarily implement Risk Management and Risk Assessment as part of their Information Security Management System. Finally, many small organizations do not implement them at all (e.g. SMEs, large organizations in the area of commerce).

2. *Absence of a "common language" in the area of Risk Management to facilitate communication of stakeholders*: In the relevant literature (e.g. national or international standards, tools, good practices etc.) Risk Management terms are used with different meanings. Similarly, experts in the area of Risk Management and Risk Assessment use often different definitions for relevant terms. The use of differentiated terminology aggravates the comparability of the achieved results, used methods and tools.

3. *Lack of surveys on existing methods, tools and good practices*: Although many methods and tools are available in this domain, no inventories do exist that are structured according to a set of common properties (enabling thus comparability). Organizations tend to proceed with costly feasibility studies on the identification of characteristics of existing methods and tools in Risk Management and Risk Assessment.

[1] As such Risk Management is performed continuously, or at least on demand, e.g. when new security incidents are registered or components (Hardware, Software) are going to be purchased, developed, deployed, etc.

4. *Lack of interoperability of Risk Management solutions; difficulties in integration of Risk Management/Risk Assessment with corporate governance*: In current time, Information Technology Risk Management and Risk Assessment cannot be considered in isolation. Both multiple methods and multiple application domains of Risk Management may co-exist (e.g. in the area of operational risks [BASEL II], [SOX]). This generates the need to integrate IT Risk Management and Risk Assessment both with existing methods/standards in the areas of Information Technology and operational risks and implement them as a whole within the organization.

The main purpose of this document is to contribute towards the points 1 and 2 mentioned above. In doing so it presents processes and operational cycles pertinent to Risk Management and proposes guidelines that can improve the effectiveness of their implementation. Chapters 3 to 9 address these points by positioning Risk Management and by describing its underlying processes.

A further purpose of this document is to contribute to point 3 above, by providing an initial survey on existing approaches by means of inventories[2] of existing methods and tools. These inventories will be maintained by ENISA in the future and they are presented in chapters 10 and 11. Detailed information on the inventories is provided in annexes attached to this document (s. annex III and annex V).

Finally, point 4 together with further emerging issues of Risk Management and Risk Assessment are addressed by means of a road map describing possible future actions in these areas. The road map is presented in chapter 12.

It is worth mentioning, that this report contains information delivered by an ad hoc Working Group established by ENISA in the area of Risk Management / Risk Assessment [ENISA-WG]. When appropriate this information has been integrated into the present text, while some of it is included in the attached inventories (esp. in the inventory of methods in Annex II).

Since ENISA's focus is on information and network security, this document mainly concentrates on Information Security (IS) Risk Management. If not otherwise noted, the terms Information Security Risk Management and Risk Management will be used in this document interchangeably.

The exact structure and purpose of this document is presented in the following chapter (s. chapter 2).

[2] The ENISA inventory is an **open** list with methods and tools. In its current version, the ENISA inventory is not exhaustive. It rather contains methods and tools from an initial assessment performed by the ENISA Working Group composed of European experts in the related field. Methods and tools not included in the current inventories can be considered for later versions. ENISA works on a process that will allow maintenance of the inventories (i.e. submission and insertions of new items, deletion of existing ones, etc.).

Note for the paper version of this document: This document is a static image of a dynamically evolving information base that in the near future will be implemented by means of a Web Site. The dynamic document will evolve over time and will include:

- additional methods/tools to be assessed later (expected by the end of 2006);
- examples provided by ENISA for instantiations of various processes of Risk Management (expected by the end of 2006);
- demonstrations of how to apply presented Risk Management processes in practice (expected by during 2007);
- examples on how to integrate Risk Management processes with other processes (expected by the middle of 2007);
- further aspects emerging from the elaboration on the open issues formulated in this document (continuously).

2 Structure and target groups of this document

The structure of the present document is as presented in Figure 1. The main part (s. box tagged as "*Risk Management/Risk Assessment Implementation Principles*") describes the main characteristics of processes and activities pertinent to Risk Management and Risk Assessment. Generally speaking, this box represents the present report. The annexes attached to this document constitute the inventory of methods and of tools, as well as a glossary of terms used within this document. Via references, the logical relationships have been implemented in this document (depicted in the figure by the yellow arrows).

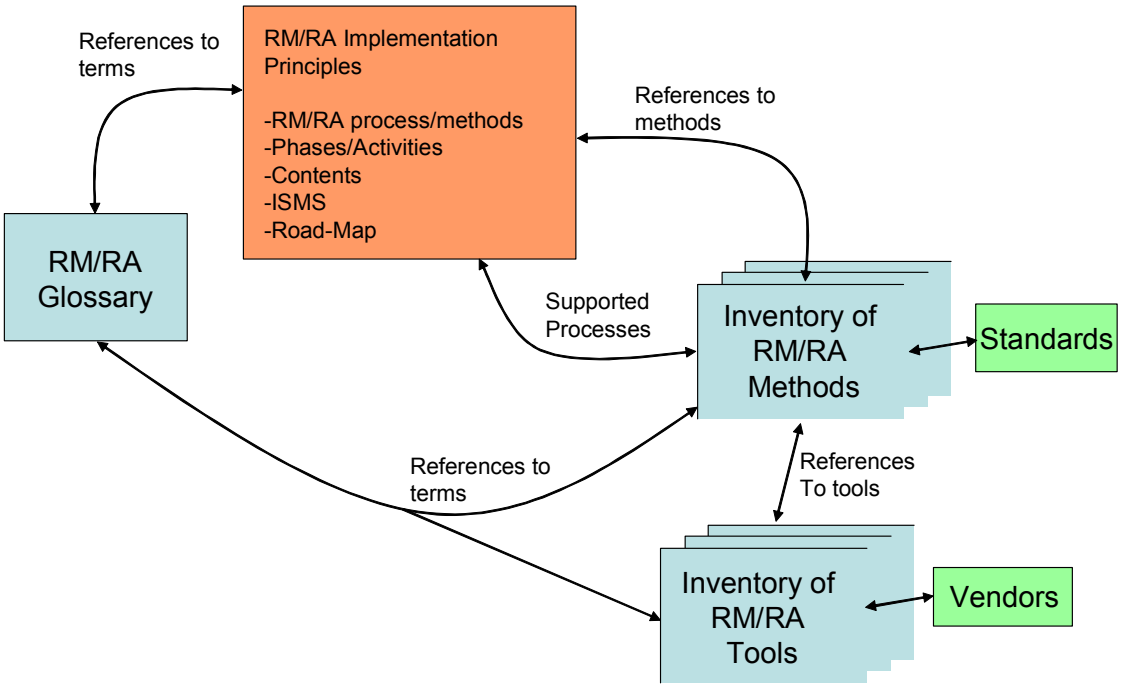

Figure 1: Structure of the present document

The target group for this document is composed of security and IT experts but also interested individuals seeking for a reference to Risk Management processes, activities and terminology. For all target groups, this document can be considered as a resource for generating awareness in the areas of Risk Management and Risk Assessment (esp. chapters 3 to 9).

Furthermore, the attached inventories offer concise information on existing methods and tools that can facilitate rapid identification of their key characteristics (see chapters 10 and 11, as well as annex III, annex V). This can be a valuable aid in the process of selection of appropriate components for the implementation of a Risk Management process within an organization. To this extend, the attached inventories serve as resource for the promotion of existing methods and tools.

Finally, the ENISA road-map reveals current and future trends in the area of Risk Management, thus giving an idea of future demand and developments in that area (see chapter 12).

Detailed inventories (both for methods and tools), together with the description of the templates used and the glossary developed are attached as annexes to this document. An electronic version of this document will be available by means of a dedicated web-site.

Further, this document can serve as:

- a generic description of processes and activities implementing Information Security Risk Management/Risk Assessment;

- a consolidated set of references to be used in future work. For this purpose, the glossary attached to this document will be continuously maintained. It is worth mentioning, that the developed glossary will comprise part of a wider glossary on security terms to be developed by ENISA;

- an initial document base to be possibly expanded in the future with aspects such:

    - process integration by means of examples of integrating Risk Management with other operative or product processes;
    - examples of organizational implementations of Risk Management processes and activities;
    - comparability and interoperability issues among various methods;
    - material that can be used for demonstration or training purposes.

3 Positioning Risk Management and Risk Assessment

Risk Management and Risk Assessment are major components of Information Security Management (ISM). Although they are widely known, a wide range of deviating definitions of Risk Management and Risk Assessment are found in the relevant literature [ISO13335-2], [NIST], [ENISA Regulation]. In this chapter a consolidated view of Risk Management and Risk Assessment is presented. For the sake of this discussion, two approaches to presenting Risk Management and Risk Assessment, mainly based on OCTAVE [OCTAVE] and ISO 13335-2 [ISO13335-2] will be considered. Nevertheless, when necessary, structural elements that emanate from other perceptions of Risk Management and Risk Assessment are also used (e.g. consideration of Risk Management and Risk Assessment as counterparts of Information Security Management System, as parts of wider operational processes, etc. [WG-Deliverable 3], [Ricciuto]).

It seems to be generally accepted by Information Security experts, that Risk Assessment is part of the Risk Management process. After initialization, Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. This view of the relationship of Risk Management to Risk Assessment is depicted in Figure 2 as adopted from OCTAVE [OCTAVE].

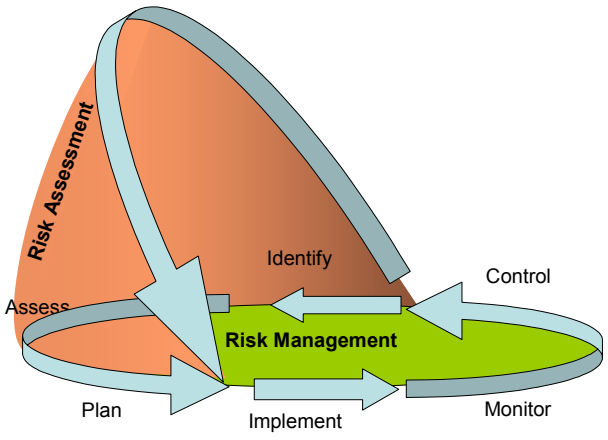

Figure 2: The relationship between Risk Management and Risk Assessment

It is worth mentioning, that in this figure both Risk Management and Risk Assessment are presented as processes, that is, as sequences of activities (s. arrows in Figure 2).

Various standards and good practices exist for the establishment of these processes (e.g. through structuring, adaptation, re-configuration etc.). In practice, organizations tend to generate their own instantiations of these methods, in a form most suitable for a given organizational structure, business area or sector. In doing so, national or international standards (or combination of those) are taken as a basis, whereas existing security mechanisms, policies and/or infrastructure are adapted one-by-one. In this way, new *good practices* for a particular sector are created. Some representative examples of tailored methods/good practices are:

- a method based on a native national standard (e.g. [IT-Grund]);
- a method based on an native international standard (e.g. [ISO13335-2]);
- a method based on a de facto standard (e.g. [OCTAVE]);
- a method based on a sector standard (e.g. [SIZ-DE]);
- a method based on an individual basic protection profile for the IT-systems of an organization (e.g. [SIZ-PP]);
- adoption of an already existing risk analysis of similar systems (e.g. based on an existing Protection Profiles according to Common Criteria [CC]).

In practice, combinations of the above examples are very common.

For the sake of the presentation within this document, the assumption is made, that the Risk Management life-cycle presented in Figure 2 (i.e. plan, implement, monitor, control, identify, assess), refers solely to **risks**. Similar activities that might be necessary within the Information Security Management process are considered to apply to **operational** aspects related to the implementation and control of security measurements (see also ISMS scope in chapter 3.1.3).

Even although organizations tend to use a single method for Risk Management, multiple methods are typically be used in parallel for Risk Assessment. This is because different Risk Assessment methods might be necessary, depending on the nature of the assessed system (e.g. structure, criticality, complexity, importance, etc.).

Through a series of activities, ENISA has established inventories of existing Risk Management and Risk Assessment methods and tools in Europe (also referred to as *products* in this document). Any of these products can be used for the instantiation of both the Risk Management and Risk Assessment processes mentioned in Figure 2 above. The contents of these inventories are discussed in chapters 10 and 11 and the inventories themselves are attached to this document as annexes (s. annex III and annex V).

It should be noted that a more detailed representation of Risk Management and Risk Assessment is given in ISO 13335-2 [ISO13335-2]. In general, the contents of Risk Management and Risk Assessment processes as described in this document are compatible with ISO 13335. In the future, detailed examples of how to adapt the processes presented to existing business and IT-needs by means of demonstrators will be

given. The generation of such material will be part future work at ENISA in form of demonstrators (s. chapter 12.3).

A detailed discussion on the processes of Risk Management and Risk Assessment is presented in chapter 4 to 9).

3.1 Risk Management within an Information Security Management System (ISMS)

Within this section the content and structure of Information Security Management Systems (ISMS) are explained and the position of Risk Management within such frameworks is shown. This will clarify the value of Risk Management within the ISMS. Further, an overview of existing interfaces with other security activities and results that provide/consume information to/from Risk Management will be presented.

3.1.1 The need for ISMS

Security experts say and statistics confirm that:

- information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- security depends on people more than on technology;
- employees are a far greater threat to information security than outsiders;
- security is like a chain. It is as strong as its weakest link;
- the degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- security is not a status or a snapshot but a running process.

These facts inevitably lead to the conclusion that:

Security administration is a management and NOT a purely technical issue

Therefore the establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks. Furthermore such a company will be capable of successfully addressing information confidentiality, integrity and availability requirements which in turn have implications for:

- business continuity;
- minimization of damages and losses;
- competitive edge;
- profitability and cash-flow;
- respected organization image;

- legal compliance.

3.1.2 Critical success factors for ISMS

To be effective, the ISMS must:

- have the continuous, unshakeable and visible support and commitment of the organization's top management;
- be managed centrally, based on a common strategy and policy across the entire organization;
- be an integral part of the overall management of the organization related to and reflecting the organization's approach to Risk Management, the control objectives and controls and the degree of assurance required;
- have security objectives and activities be based on business objectives and requirements and led by business management;
- undertake only necessary tasks and avoiding over-control and waste of valuable resources;
- fully comply with the organization philosophy and mindset by providing a system that instead of preventing people from doing what they are employed to do, it will enable them to do it in control and demonstrate their fulfilled accountabilities;
- be based on continuous training and awareness of staff and avoid the use of disciplinary measures and "police" or "military" practices;
- be a never ending process;

Establishing an ISMS, involves:

- establishing the necessary Management Framework;
- implementing selected controls;
- documenting the system;
- applying proper documentation control;
- maintaining records demonstrating compliance.

3.1.3 The ISMS Framework

Chief objective of Information Security Management is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, Information Security Management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e. availability of services, preservation of data confidentiality and integrity etc.).

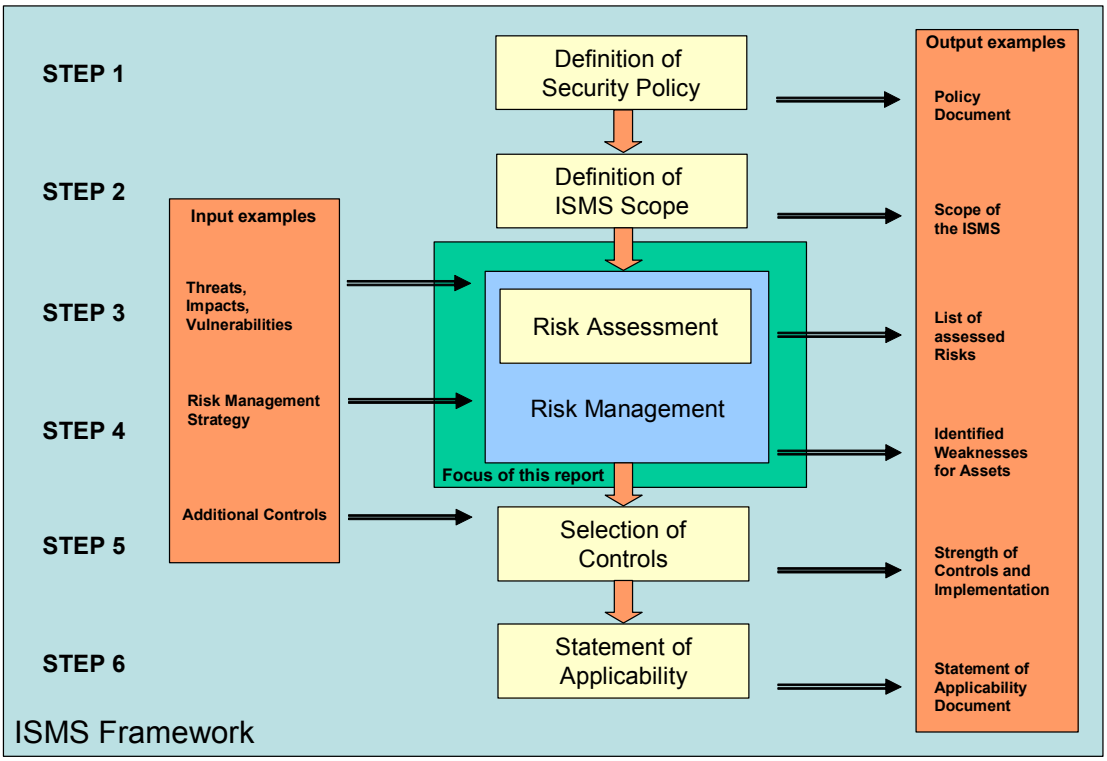

Figure 3: A possible ISMS Framework (based on ISO 17799)

It is not only size but in particular the specific business activities of an organization that dictate its security related requirements on a legal, regulatory and operational level.

Small businesses with limited information systems infrastructure, whose operation does not demand handling, storage and processing of personal or confidential data, usually face minor risks or risks with lower likelihood or impact. These organizations are more likely not to maintain independent ISMS and usually deal with information security risks ad-hoc or as part of a wider Risk Management process.

Larger organizations and organizations such as banks and financial institutes, telecommunication operators, hospital and health institutes and public or governmental bodies have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmost attention and priority to information security risks.

Under these circumstances the development and implementation of a separate and independent management process namely an Information Security Management System is the one and only alternative.

As shown in Figure 3, the development of an ISMS framework entails the following 6 steps:

1. Definition of Security Policy,
2. Definition of ISMS Scope,
3. Risk Assessment (as part of Risk Management),
4. Risk Management,
5. Selection of Appropriate Controls and
6. Statement of Applicability

Steps 3 and 4, the Risk Assessment and Management process, comprise the heart of the ISMS and are the processes that "transform" on one hand the rules and guidelines of security policy and the targets; and on the other to transform objectives of ISMS into specific plans for the implementation of controls and mechanisms that aim at minimizing threats and vulnerabilities. It is worth mentioning, that steps 3 and 4 are considered as a single entity, namely Risk Management.

The processes and activities related to the steps 5 and 6 do not concern information risks. They are rather related to the operative actions required for the technical implementation, maintenance and control of security measurements.

Appropriate controls may either be derived from existing (exhaustive) sets of controls or mechanisms, usually included in information security standards (e.g. [ISO 17799]) and guidelines, or be the outcome of a combination or adaptation of proposed controls to the specific organizational requirements or operational characteristics.

In both cases, step 6 is the documented mapping of the identified risks, applied to the specific organization with the technical implementation of security mechanisms the organization has decided to deploy.

Finally it should be mentioned that although the ISMS is a recurring process as a whole, in most of the types of organizations mentioned above, steps 1 and 2 recur on a longer cycle than steps 3,4,5 and 6. This is mainly because the establishment of a security policy and the definition of the ISMS scope are more often management and (to a certain extent) strategic issues while the Risk Management process is in the end an "everyday" operational concern.

4 Risk Management Processes

The effectiveness of Risk Management strongly depends on the degree to which it succeeds in becoming a part of an organization's culture, i.e. its philosophy, practices and business processes. In this way, Risk Management is the responsibility of everyone in the organization.

The design and implementation of a Risk Management process in a particular organization is always influenced by:

- the organization mission and objectives;
- its products and services;
- its management and operation processes;
- specific practices employed;
- the local physical, environmental and regulatory conditions.

The impact that these factors have on the implementation of Risk Management, is presented in more detail in the following chapters.

As opposed to the evaluation of future risks, Risk Management as treated in this document refers to the management of current known risks. In this respect, Risk Management (including methods and tools) is based on empirical and/or statistical values drawn form known attacks and incidents of the past.

The anticipation of future risks, also referred to as "*Emerging Risks*" [Emerging Risk ENISA], [Emerging Risk IPTS], will be addressed by ENISA at a later time. Mainly, Emerging Risks are addressed on the basis of virtual future scenarios. It is worth mentioning, that the effectiveness and quality of assessments of Emerging Risks depends on the plausibility and practicability of the asserted future scenarios. At the time being, ENISA initializes work in the area of Emerging Risks and generates a road-map for the following years.

4.1 Overview of the Risk Management Processes

The presentation of Risk Management processes in this chapter is a consolidated overview of relevant content found in the corresponding literature ([WG-Deliverable 3], [ISO 13335-2], [Ricciuto]). As mentioned above, the presented structure is compatible with the ISO Standard 13335.

In the present document Risk Management is considered to be the umbrella under which several processes / activities concerning the identification, mitigation, management and control of risks take place. For the sake of the presentation, an integrated view of Risk Management is presented in terms of a "big picture", i.e. the five processes and their activities (s. Figure 4). Furthermore, this figure shows possible interfaces among the processes presented.

In practice, any of the Risk Management processes can be used as an entry point to the Risk Management process or can be performed in isolation. Many organizations, for example, perform Risk Treatment without the performance of Risk Assessment or without the prior establishment of a Corporate Risk Management Strategy. Others might perform Risk Assessment and then proceed directly with other activities of ISMS.

The ideal sequence for the performance of the processes of Risk Management is to start with the establishment of a Corporate Risk Management Strategy and proceed according to the orange cyclic arrow as indicated in the figure, whereas mutual interactions between the processes might also be performed (e.g. performance of Risk Assessment after a Risk Acceptance).

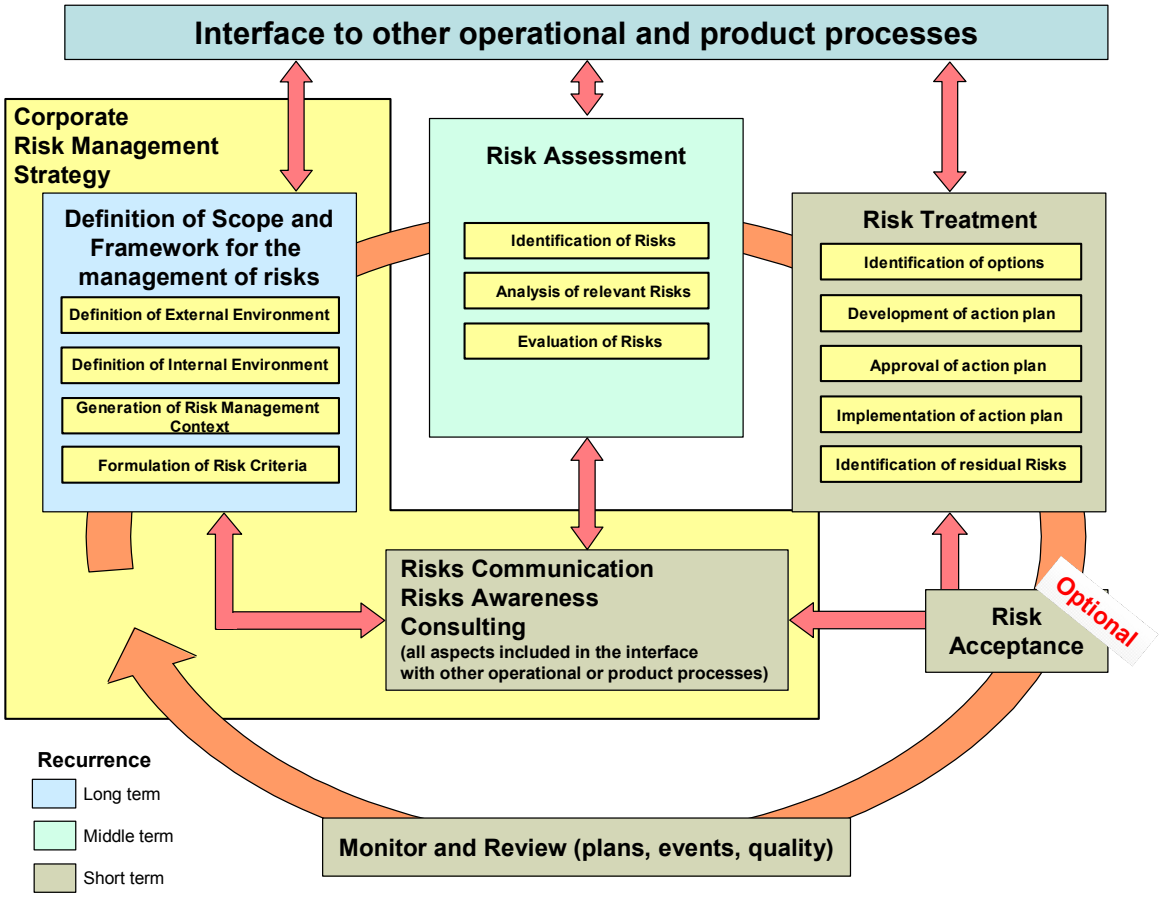

Figure 4: Overall cycle of a Risk Management process

It is worth mentioning, that no effective Risk Management system can be established in an organization, if it lacks such interfaces and especially to other relevant operational or product processes (s. box at the top of the figure). In its future work on Risk Management, ENISA will elaborate examples to demonstrate ways to integrate Risk Management activities in important operational processes (e.g. procurement, software

development and test) as well as product processes (e.g. user help desks, incidents reporting).

In this chapter an overview Risk Management is presented. For the definition of Risk Management itself, the ENISA definition is adopted:

- *Risk Management* is the process**,** distinct from Risk Assessment, of weighing policy alternatives in consultation with interested parties, considering Risk Assessment and other legitimate factors, and selecting appropriate prevention and control options.
  (Definition provided in ENISA Regulation [ENISA Regulation])

Risk Management is considered as consisting of the five main processes shown in the figure above: *Definition of Scope*, *Risk Assessment*, *Risk Treatment*, *Risk Communication* and *Monitor and Review*. It is worth mentioning, that the two processes Definition of Scope and Risk Communication are considered to make up the *Risk Management Strategy* (represented in Figure 4 by the yellow box).

For the above mentioned processes of Risk Management the following definitions[3] are used:

- *Definition of Scope*: Process for the establishment of global parameters for the performance of Risk Management within an organization. Within the definition of scope for Risk Management, both internal and external factors have to be taken into account.
  (ENISA)

- *Risk Assessment*: A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation.
  (Definition adopted from ENISA Regulation with some adaptation concerning the name and number of the foreseen steps[4])

- *Risk Treatment*: Process of selection and implementation of measures to modify risk.
  - Risk treatment measures can include avoiding, optimizing, transferring or retaining risk

  (Definition adopted from ISO/IEC Guide 73)

[3] The definitions used within this document can be found in the attached glossary (s. page Glossary on 53). These definitions have been adopted from different sources (including ISO/IEC Guide 73 [Guide 73], ENISA Regulation [ENISA Regulation], NIST [NIST] etc) and adapted accordingly.
[4] The ENISA Regulation [ENISA Regulation] foresees four steps instead of three mentioned in the present definition. In this document the names of the activities have been changed and the step "threat characterization" has been eliminated, as it is considered to be part of Risk Identification (s. section 6.1).

- *Risk Communication*: A process to exchange or share information about risk between the decision-maker and other stakeholders inside and outside an organization (e.g. departments and outsourcers respectively).
    - The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

    (Definition adopted from ISO/IEC Guide 73)

- *Monitor and Review*: A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions.
  (ENISA)

In the relevant literature, a further process of Risk Management is often mentioned, namely *Risk Acceptance*. In this document Risk Acceptance is considered as being an *optional* process, positioned between Risk Treatment and Risk Communication. This process is seen as an optional one, because it can be covered by both Risk Treatment and Risk Communication processes. This can be achieved by communicating the outcome of Risk Treatment to the management of the organization. A reason for deliberately mentioning Risk Acceptance is to achieve the necessary management attention for this, otherwise purely communicative activity. Risk Acceptance can be defined as follows:

- *Risk Acceptance*: Decision to accept a risk by the responsible management of the organization.
    - Risk acceptance depends on risk criteria defined within the process Definition of Scope

    (Definition adopted from ISO/IEC Guide 73 with some modification)

These above mentioned processes are presented in the sections of this chapter in detail.

5 The Corporate Risk Management Strategy

Risk Management Strategy is an integrated business process that incorporates all of the Risk Management processes, activities, methodologies and policies adopted and carried out in an organization. The Risk Management strategy sets the parameters for the entire Risk Management and is usually released by the executive management of an organization.

As depicted in Figure 4, Risk Management Strategy consists of two processes, one setting the framework for the entire Risk Management and the other setting the communication channels in the organization (see yellow box embracing *Definition of Scope* and *Risk*

Communication). In the forthcoming sections the components of Risk Management Strategy will be analyzed.

5.1 Risk Communication, Risk Awareness and Consulting

As mentioned above, it is essential for Risk Management to become part of the organization's culture. Therefore communicating and creating awareness of relative issues across the organization at each step of the Risk Management process are very important.

Communication should by all means involve an open discussion with all stakeholders with efforts focused on consultation and development of common understanding, rather than on a one way flow of information from the decision maker to the other stakeholders.

Risk Management can and will be enhanced by parties and individuals understand each other's perspectives and who are consulted in a timely fashion, where appropriate. Stakeholders, like every human being, tend to make judgments about risk based on their perceptions. These can vary due to differences in values, needs, assumptions, concepts and concerns, as they relate to the risks or the issues under discussion. Since the views of stakeholders can have a significant impact on the decisions made, it is important that possible variations in their perceptions of risk be identified, recorded and addressed in the decision making process. In the long term, ENISA will contribute to the generation of qualitative criteria aiming at the creation of balanced estimations about assessed risks among various experts using various methods and tools.

External communication and consulting by specialized consultants, as well as exchange of information and cooperation with other organizations should also be planned and implemented on a regular basis. The exchange of this knowledge and experience can prove extremely helpful for addressing issues related to both the risks and the process to manage these risks, leading thus to a view on risks that is free from subjective estimations. Furthermore, involving external personnel in such activities contributes towards the renewal of available know-how and risk perception[5].

5.2 Definition of Scope and Framework

By establishing the framework for the management of risks, the basic parameters within which risks must be managed are defined. Consequently, the scope for the rest of the Risk Management process is also set. It includes the definition of basic assumptions for the organization's external and internal environment and the overall objectives of the Risk Management process and activities. Although the definition of scope and framework are fundamental for the establishment of Risk Management, they are independent from

[5] It is often the case that "established" practices lead to isolated or narrow observation of the status quo of the security. External personnel contribute in bringing in "fresh air" by means of additional viewpoints in the evaluation of risks.

the particular structure of the management process, methods and tools to be used for the implementation.

In order to define an efficient framework it is important to:

- understand the background of the organization and its risks (e.g. its core processes, valuable assets, competitive areas etc.);
- evaluate the Risk Management activities being undertaken so far;
- develop a structure for the Risk Management initiatives and controls (countermeasures, security controls etc.) to follow.

This approach is useful for:

- clarifying and gaining common understanding of the organizational objectives;
- identifying the environment in which these objectives are set;
- specifying the main scope and objectives for Risk Management, applicable restrictions or specific conditions and the outcomes required;
- developing a set of criteria against which the risks will be measured;
- defining a set of key elements for structuring the risk identification and assessment process.

5.2.1 Definition of external environment

This step includes the specification of the external environment in which the organization operates and the definition of the relationship between this environment and the organization itself.

The external environment typically includes:

- the local market, the business, competitive, financial and political environment;
- the law and regulatory environment;
- social and cultural conditions;
- external stakeholders.

It is also very important that both the perceptions and values of the various stakeholders and any externally generated threats and/or opportunities are properly evaluated and taken into consideration.

5.2.2 Definition of internal environment

As in every significant business process, the most critical prerequisite is to understand the organization itself.

Key areas that must be evaluated in order to provide a comprehensive view of the organization's internal environment include:

- key business drivers (e.g. market indicators, competitive advances, product attractiveness, etc.);
- the organization's strengths, weaknesses, opportunities and threats;
- internal stakeholders;
- organization structure and culture;
- assets in terms of resources (such as people, systems, processes, capital etc);
- goals and objectives and the strategies already in place to achieve them.

5.2.3 Generating the Risk Management context

In business terms, Risk Management as a process should provide a balance between (all kinds of) costs, benefits and opportunities. Therefore, it is necessary to draw the appropriate framework and to correctly set the scope and boundaries of the Risk Management process.

Setting the Risk Management context involves defining the:

- organization, process, project or activity (to be assessed) and establishing its goals and objectives;
- duration of the project, activity or function;
- full scope of the Risk Management activities to be carried out specifying any including inclusions and exclusions;
- roles and responsibilities of various parts of the organization participating in the Risk Management process;
- dependencies between the project or activity and other projects or parts of the organization;

5.2.4 Formulation of risk criteria

The criteria by which risks will be evaluated have to be decided and agreed. Deciding whether risk treatment is required, is usually based on operational, technical, financial, regulatory, legal, social, or environmental, criteria or combinations of them. The criteria should be in line with the scope and framework defined above. Furthermore they should be closely related to the organization's internal policies and procedures and support its goals and objectives.

Important criteria, to be considered, are:

- impact criteria and the kinds of consequences that will be considered;
- criteria of likelihood;

- the rules that will determine whether the risk level is such that further treatment activities are required.

It is very common, that criteria identified during these steps are further developed or even modified during later phases of the Risk Management process.

6 Risk Assessment

Every organization is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfillment of its objectives. Identification, analysis and evaluation of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. It has to be noted, that Risk Assessment is a process that in many cases is not (at least not adequately) performed, even if Risk Management is implemented. It is one of the main objectives of ENISA to generate awareness of this fact, but also to facilitate use of Risk Assessments by providing practical examples (see also chapter 12.3).

For insurance companies, the performance of Risk Assessments is in general of significant importance and in particular concerning IT risks for current and potential customers.

6.1 Identification of Risks

This is the phase where threats, vulnerabilities and the associated risks are identified. This process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is very important that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organization.

The first step is to generate a comprehensive list of sources of threats, risks and events that might have an impact on the achievement of each of the objectives as identified in the Definition of Scope and Framework (s section 5.2). These events might prevent, degrade, delay or enhance the achievement of those objectives.

In general, a risk can be related to or characterized by

(a) it's origin
(e.g. threat agents like hostile employees or employees not properly trained, competitors, governments etc.)

(b) a certain activity, event or incident (i.e. threat)
(e.g. unauthorized dissemination of confidential data, competitor deploys a new marketing policy, new or revised data protection regulations, an extensive power failure)

(c) its consequences, results or impact
(e.g. service unavailability, loss or increase of market/profits, increase in regulation increase or decrease in competitiveness, penalties, etc.)

(d) a specific reason for its occurrence
(e.g. system design error, human intervention, prediction or failure to predict competitor activity)

(e) protective mechanisms and controls (together with their possible lack of effectiveness)
(e.g. access control and detection systems, policies, security training, market research and surveillance of market)

(f) time and place of occurrence
(e.g. during extreme environmental conditions there is a flood in the computer room)

Good quality information and thorough knowledge of the organization and its internal and external environment are very important in identifying risks. Historical information about this or similar organizations (competitors or not) may also prove very useful as they can lead to safe predictions about current and evolving issues that have not yet faced by the organization.

Identifying what may happen is rarely sufficient. The fact that there are many ways an event can occur makes it important to study all possible and significant causes and scenarios. Methods and tools used to identify risks and their occurrence include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques.

In selecting a risk identification methodology, the following techniques should be considered:

- team-based brainstorming where workshops can prove effective in building commitment and making use of different experiences;
- structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability studies,6 and operational modeling;
- for less clearly defined situations, such as the identification of strategic risks, processes with a more general structure such as ‘what-if’ and scenario analysis could be used.

[6] The HAZOP [HAZOP] process is based on the principle that a team approach to hazard analysis will identify more problems than when individuals working separately combine results. The HAZOP team is made up of individuals with varying backgrounds and expertise. The expertise is brought together during HAZOP sessions and through a collective brainstorming effort that stimulates creativity and new ideas, a thorough review of the process under consideration is made.

6.2 Analysis of relevant Risks

Risk analysis is the phase where the level of the risk and its nature are assessed and understood. This information is the first input to decision makers on whether risks need to be treated or not and what is the most appropriate and cost-effective risk treatment methodology.

Risk analysis involves:

- thorough examination of the risk sources;
- their positive and negative consequences;
- the likelihood that those consequences may occur and the factors that affect them;
- assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks (these controls may derive from a wider set of standards, controls or good practices selected according to a an applicability statement and may also come from previous risk treatment activities.)

The level of risk can be estimated by using statistical analysis and calculations combining impact and likelihood. Any formulas and methods for combining them must be consistent with the criteria defined when establishing the Risk Management context (s. section 5.2.3). This is because an event may have multiple consequences and affect different objectives, therefore consequences and likelihood need to be combined to calculate the level of risk. If no reliable or statistically reliable and relevant past data is available (kept for e.g. an incident database), other estimates may be made as long as they are appropriately communicated and approved by the decision makers.

Information used to estimate impact and likelihood usually comes from:

- past experience or data and records (e.g. incident reporting),
- reliable practices, international standards or guidelines,
- market research and analysis,
- experiments and prototypes,
- economic, engineering or other models,
- specialist and expert advice.

Risk analysis techniques include

- interviews with experts in the area of interest and questionnaires,
- use of existing models and simulations.

Risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources. Analysis may be qualitative, semi-quantitative or quantitative or a combination of these. In any case, the

type of analysis performed should, as stated above, be consistent with the criteria developed as part of the definition of the Risk Management context (see section 5.2.3).

A short description of the above-mentioned types of analysis types is as follows:

- Qualitative analysis

  In qualitative analysis, the magnitude and likelihood of potential consequences are presented and described in detail. The scales used can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks.

  Qualitative analysis may be used:

  - as an initial assessment to identify risks which will be the subject of further, detailed analysis;
  - where non-tangible aspects of risk are to be considered (e.g. reputation, culture, image etc.)
  - where there is a lack of adequate information and numerical data or resources necessary for a statistically acceptable quantitative approach.

- Semi-quantitative analysis

  In semi-quantitative analysis the objective is to try to assign some values to the scales used in the qualitative assessment. These values are usually indicative and not real, which is the prerequisite of the quantitative approach.

  Therefore, as the value allocated to each scale is not an accurate representation of the actual magnitude of impact or likelihood, the numbers used must only be combined using a formula that recognizes the limitations or assumptions made in the description of the scales used.

  It should be also mentioned that the use of semi-quantitative analysis may lead to various inconsistencies due to the fact that the numbers chosen may not properly reflect analogies between risks, particularly when either consequences or likelihood are extreme.

- Quantitative analysis

  In quantitative analysis numerical values are assigned to both impact and likelihood. These values are derived from a variety of sources. The quality of the entire analysis depends on the accuracy of the assigned values and the validity of the statistical models used.

Impact can be determined by evaluating and processing the various results of an event or by extrapolation from experimental studies or past data. Consequences may be expressed in various terms of

- monetary
- technical
- operational
- human

impact criteria.

As it is made clear from the above analysis, the specification of the risk level is not unique. Impact and likelihood may be expressed or combined differently, according to the type of risk and the scope and objective of the Risk Management process.

6.3 Evaluation of Risks

During the risk evaluation phase decisions have to be made concerning which risks need treatment and which do not, as well as concerning on the treatment priorities. Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the Risk Management context (i.e. in the risk criteria identification stage). It is important to note that in some cases the risk evaluation may lead to a decision to undertake further analysis.

The criteria used by the Risk Management team have to also take into account the organization objectives, the stakeholder views and of course the scope and objective of the Risk Management process itself.

The decisions made are usually based on the level of risk but may also be related to thresholds specified in terms of:

- consequences (e.g. impacts),
- the likelihood of events,
- the cumulative impact of a series of events that could occur simultaneously.

7 Risk Treatment

According to its definition, Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. The measures (i.e. security measurements) can be selected out of sets of security measurements that are used within the Information Security Management System (ISMS) of the organization. At this level, security measurements are verbal descriptions of various security functions that are implemented technically (e.g. Software or Hardware components) or organizationally (e.g. established procedures).

7.1 Identification of options

Having identified and evaluated the risks, the next step involves the identification of alternative appropriate actions for managing these risks, the evaluation and assessment of their results or impact and the specification and implementation of treatment plans.

Since identified risks may have varying impact on the organization, not all risks carry the prospect of loss or damage. Opportunities may also arise from the risk identification process, as types of risk with positive impact or outcomes are identified.

Management or treatment options for risks expected to have positive outcome include:

- starting or continuing an activity likely to create or maintain this positive outcome;
- modifying the likelihood of the risk, to increase possible beneficial outcomes;
- trying to manipulate possible consequences, to increase the expected gains;
- sharing the risk with other parties that may contribute by providing additional resources which could increase the likelihood of the opportunity or the expected gains;
- retaining the residual risk.

Management options for risks having negative outcomes look similar to those for risks with positive ones, although their interpretation and implications are completely different. Such options or alternatives might be:

- to avoid the risk by deciding to stop, postpone, cancel, divert or continue with an activity that may be the cause for that risk;
- to modify the likelihood of the risk trying to reduce or eliminate the likelihood of the negative outcomes;
- to try modifying the consequences in a way that will reduce losses;
- to share the risk with other parties facing the same risk (insurance arrangements and organizational structures such as partnerships and joint ventures can be used to spread responsibility and liability); (of course one should always keep in mind that if a risk is shared in whole or in part, the organization is acquiring a new risk, i.e. the risk that the organization to which the initial risk has been transferred may not manage this risk effectively.)
- to retain the risk or its residual risks;

In general, the cost of managing a risk needs to be compared with the benefits obtained or expected. During this process of cost-benefit judgments, the Risk Management context established in the first process (i.e. Definition of Scope and Framework, s. section 5.2) should be taken into consideration. It is important to consider all direct and indirect costs and benefits whether tangible or intangible and measured in financial or other terms.

More than one option can be considered and adopted either separately or in combination. An example is the effective use of support contracts and specific risk treatments followed by appropriate insurance and other means of risk financing.

In the event that available resources (e.g. the budget) for risk treatment are not sufficient, the Risk Management action plan should set the necessary priorities and clearly identify the order in which individual risk treatment actions should be implemented.

7.2 Development of the action plan

Treatment plans are necessary in order to describe how the chosen options will be implemented. The treatment plans should be comprehensive and should provide all necessary information about:

- proposed actions, priorities or time plans,
- resource requirements,
- roles and responsibilities of all parties involved in the proposed actions,
- performance measures,
- reporting and monitoring requirements.

Action plans should be in line with the values and perceptions of all types of stakeholders (e.g. internal organizational units, outsourcing partner, customers etc.). The better the plans are communicated to the various stakeholders, the easier it will be to obtain the approval of the proposed plans and a commitment to their implementation.

7.3 Approval of the action plan

As with all relevant management processes, initial approval is not sufficient to ensure the effective implementation of the process. Top management support is critical throughout the entire life-cycle of the process. For this reason, it is the responsibility of the Risk Management Process Owner to keep the organization's executive management continuously and properly informed and updated, through comprehensive and regular reporting.

7.4 Implementation of the action plan

The Risk Management plan should define how Risk Management is to be conducted throughout the organization. It must be developed in a way that will ensure that Risk Management is embedded in all the organization's important practices and business processes so that it will become relevant, effective and efficient[7].

More specifically, Risk Management should be embedded in the policy development process, in business and strategic planning, and in change management processes. It is also likely to be embedded in other plans and processes such as those for asset

[7] The integration of the Risk Management process with other operational and product processes is fundamental. ENISA plans to elaborate on this issue in the medium term based on examples with de facto process standards, such as example ITIL [ITIL].

management, audit, business continuity, environmental management, fraud control, human resources, investment and project management.

The Risk Management plan may include specific sections for particular functions, areas, projects, activities or processes. These sections may be separate plans but in all cases they should be consistent with the organization's Risk Management strategy (which includes specific RM policies per risk area or risk category).

The necessary awareness of and commitment to Risk Management at senior management levels throughout the organization is mission critical and should receive close attention by:

- obtaining the active ongoing support of the organization's directors and senior executives for Risk Management and for the development and implementation of the Risk Management policy and plan;
- appointing a senior manager to lead and sponsor the initiatives;
- obtaining the involvement of all senior managers in the execution of the Risk Management plan.

The organization's board should define, document and approve its policy for managing risk, including objectives and a statement of commitment to Risk Management. The policy may include:

- the objectives and rationale for managing risk;
- the links between the policy and the organization's strategic plans;
- the extent and types of risk the organization will take and the ways it will balance threats and opportunities;
- the processes to be used to manage risk;
- accountabilities for managing particular risks;
- details of the support and expertise available to assist those involved in managing risks;
- a statement on how Risk Management performance will be measured and reported;
- a commitment to the periodic review of the Risk Management system;
- a statement of commitment to the policy by directors and the organization's executive.

Publishing and communicating a policy statement of this type demonstrates to the organization's internal and external environment the commitment of the executive board to Risk Management and clearly specifies roles and accountability on a personal level.

The directors and senior executives must be ultimately responsible for managing risk in the organization. All personnel are responsible for managing risks in their areas of control. This may be facilitated by:

- specifying those accountable for the management of particular risks, for implementing treatment strategies and for the maintenance of controls;
- establishing performance measurement and reporting processes;
- ensuring appropriate levels of recognition, reward, approval and sanction.

As it becomes apparent, the actual implementation of security measurements for the underlying IT platform is not part of this activity. Rather, the implementation of action plans is concerned with the actions to be performed to reduce the identified risks. The work necessary at the level of the technical implementation of security measures is conducted within the ISMS, that is, outside the Risk Management process.

Last but not least, an important responsibility of the top management is to identify requirements and allocate necessary resources for Risk Management. This should include people and skills, processes and procedures, information systems and databases, money and other resources for specific risk treatment activities. The Risk Management plan should also specify how the Risk Management skills of managers and staff will be developed and maintained.

7.5 Identification of residual risks

Residual risk is a risk that remains after Risk Management options have been identified and action plans have been implemented. It also includes all initially unidentified risks as well as all risks previously identified and evaluated but not designated for treatment at that time.

It is important for the organizations management and all other decision makers to be well informed about the nature and extent of the residual risk. For this purpose, residual risks should always be documented and subjected to regular monitor-and-review procedures.

8 Risk Acceptance (optional process)

Acceptance of residual risks that result from with Risk Treatment has to take place at the level of the executive management of the organization (s. definitions in chapter 4.1). To this extent, Risk Acceptance concerns the communication of residual risks to the decision makers.

Once accepted, residual risks are considered as risks that the management of the organization knowingly takes. The level and extent of accepted risks comprise one of the major parameters of the Risk Management process. In other words, the higher the accepted residual risks, the less the work involved in managing risks (and inversely).

This does not mean, however, that once accepted the risks will not change in forthcoming repetitions of the Risk Management life-cycle. Within the recurring phases and activities of the Risk Management processes (and in particular Risk Treatment as well as Monitor and Review) the severity of these risks will be measured over time. In the event that new

assertions are made or changing technical conditions identified, risks that have been accepted need to be reconsidered.

Risk Acceptance is considered as being an *optional* process, positioned between Risk Treatment and Risk Communication (s. chapter 4.1). This process is seen as an optional one, because it can be covered by both Risk Treatment and Risk Communication processes. This can be achieved by communicating the outcome of Risk Treatment to the management of the organization. One reason for explicitly mentioning Risk Acceptance is the need to draw management's attention to this issue which would otherwise merely be a communicative activity.

In the attached inventories, Risk Acceptance has been included in the assessment of methods and tools, as it might be a decision criterion for certain kinds of organizations (e.g. in the financial and insurance sector, in critical infrastructure protection etc.).

9 Monitor and Review

One of the most critical factors affecting the efficiency and effectiveness of the organization's risk management process is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. In today's continuously changing business environment, factors affecting the likelihood and consequences of a risk are very likely to change also. This is even truer for factors affecting the cost of the risk management options. It is therefore necessary to repeat the risk management cycle regularly.

To make Risk Management become a part of the organization's culture and philosophy, the organization must collect and document experience and knowledge through a consistent monitoring and review of events, treatment plans, results and all relevant records. This information, however, will be pertinent to information risks. Technical details concerning operational issues of the underlying technology have to be filtered out.

Each stage of the Risk Management process must be recorded appropriately. Assumptions, methods, data sources, results and reasons for decisions must be included in the recorded material.

Besides being an extremely valuable information asset for the organization, the records of such processes are an important aspect of good corporate governance provided of course that they are in line with:

- the legal, regulatory and business needs for records,
- the cost of creating and maintaining such records,
- the benefits of re-using information.

Finally it is very important to point out that ***Risk Management records along with all relevant documentation contain extremely critical and confidential information that should be treated with the appropriate classification level requirements.***

10 Inventory of Risk Management / Risk Assessment methods

ENISA has generated an inventory of Risk Management / Risk Assessment methods. A total 13 methods have been considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes that describe characteristics of a method. The structure of the template and the meaning of each attribute can be found in annex II.

The methods considered have been selected by the ENISA *ad hoc Working Group on technical and policy aspects of Risk Assessment and Risk Management* [ENISA-WG]. The inventory of methods is not exhaustive. Due to the composition of the ENISA Working Group (experts from eight EU member states) as well as the time available, only a limited number of methods were addressed. Therefore, this document does not contain a complete list of methods and standards dealing with IT risks.

Specific methods were deliberately excluded from the survey:

- **High-level reference documents**: documents like the ISO Guide 73 [Guide 73] are not taken into consideration.
- **Non-RA/RM methods**: methods that are not classified as RA or RM oriented, according to the definitions used.
- **Unknown methods**: some methods could not be investigated, because relevant documentation was not available to the members of the working group (e.g. Magerit from Spain).
- **General management oriented (i.e. corporate governance) methods**: for example Cobit [Cobit], Basel II [BASEL II] have been excluded due to this reason.
- **Product or system security oriented methods**: for example Common Criteria [CC] is excluded for this reason.

However, as the inventory is an **open** list, additional methods will be included in the future. For this purpose, ENISA is currently developing a process for submission of additional methods through standardization bodies/vendors, etc., as well as a process to update existing inventory entries.

The information included in the inventory of methods has been assessed by the experts of the ENISA Working Group in 2005 and reflects the status of the assessed methods at that time. In cases of newer releases it might be the case that some of the method properties described in the templates do not correspond to the current version. Through recurring assessments this information will be permanently updated.

In this chapter the considered Risk Management / Risk Assessment methods are shortly enlisted. For this purpose the text of the template attribute “description” will be used. For each method a reference to its corresponding template from the annex is given.

10.1 Austrian IT Security Handbook

The *Austrian IT Security Handbook* consists of 2 parts. Part 1 gives a detailed description of the IT security management process, including development of security policies, risk analysis, design of security concepts, implementation of the security plan and follow-up activities. Part 2 is a collection of 230 baseline security measures. A tool supporting the implementation is available as a prototype. The *Austrian IT Security Handbook* was originally developed for government organizations, and is now available for all types of business. The handbook is compliant with ISO/IEC IS 13335, the German IT-Grundschutzhandbuch and partly with ISO/IEC IS 17799.

A detailed description of Austrian IT Security Handbook can be found in the annex III (s. chapter 13)

10.2 CRAMM

CRAMM is a risk analysis method developed by the British government organization *CCTA* (Central Communication and Telecommunication Agency), now renamed zhe Office of Government Commerce (OGC). A tool having the same name supports the method: *CRAMM*. The *CRAMM* method is rather difficult to use without the *CRAMM* tool. The first releases of *CRAMM* (method and tool) were based on best practices of British government organizations. At present *CRAMM* is the UK government's preferred risk analysis method, but *CRAMM* is also used in many countries outside the UK. *CRAMM* is especially appropriate for large organizations, like government bodies and industry.

A detailed description of CRAMM can be found in the annex III (s. chapter 14)

10.3 Dutch A&K analysis

The method *Afhankelijkheids- en Kwetsbaarheidsanalyse* (*A&K analysis*) was developed in draft form by the Dutch public company *RCC*. The Dutch ministry of internal affairs completed the development in 1996 and published a handbook describing the method. The method has not been updated since that time. The *A&K analysis* is the unique and preferred method for risk analysis by Dutch government bodies since 1994. Besides the Dutch government, Dutch companies often use *A&K analysis*.

A detailed description of Dutch A&K analysis can be found in the annex III (s. chapter 15)

10.4 EBIOS

EBIOS is a comprehensive set of guides (plus a free open source software tool) dedicated to Information System risk managers. Originally developed by the French government, it is now supported by a club of experts of diverse origin. This club is a forum on Risk

Management, active in maintaining *EBIOS* guides. It produces best practices as well as application documents targeted to end-users in various contexts. *EBIOS* is widely used in the public as well as in the private sector, both in France and abroad. It is compliant with major IT security standards.

EBIOS gives risk managers a consistent and high-level approach to risks. It helps them acquire a global and coherent vision, useful for support decision-making by top managers on global projects (business continuity plan, security master plan, security policy), as well as on more specific systems (electronic messaging, nomadic networks or web sites for instance). *EBIOS* clarifies the dialogue between the project owner and project manager on security issues. In this way, it contributes to relevant communication with security stakeholders and spreads security awareness.

EBIOS approach consists of a cycle of 5 phases:

- Phase 1 deals with context analysis in terms of global business process dependency on the information system (contribution to global stakes, accurate perimeter definition, relevant decomposition into information flows and functions).
- Both the security needs analysis and threat analysis are conducted in phases 2 and 3 in a strong dichotomy, yielding an objective vision of their conflicting nature.
- In phases 4 and 5, this conflict, once arbitrated through a traceable reasoning, yields an objective diagnostic on risks. The necessary and sufficient security objectives (and further security requirements) are then stated, proof of coverage is furnished, and residual risks made explicit.

EBIOS turns out to be a flexible tool. It may produce a wide range of deliverables (*SSRS*, security target, protection profile, action plan, etc). Local standard bases (e.g.: *German IT Grundschutz*) are easily added on to its internal knowledge bases (attack methods, entities, vulnerabilities) and catalogues of best practices (*EBIOS* best practices, *ISO/IEC IS 17799*).

A detailed description of EBIOS can be found in the annex III (s. chapter 16)

10.5 ISF methods for risk assessment and risk management

The Standard of Good Practice provides a set of high-level principles and objectives for information security together with associated statements of good practice. They can be used to improve the level of security in an organization in a number of ways.
The Standard of Good Practice is split into five distinct aspects, each of which covers a particular type of environment. These are:

- Security Management (enterprise-wide)
- Critical Business Applications
- Computer Installations (‘Information Processing’ in previous versions)

- Networks ('Communications Networks' in previous versions)
- Systems Development

FIRM is a detailed methodology for the monitoring and control of information risk at the enterprise level. It has been developed as a practical approach to monitoring the effectiveness of information security. As such it enables information risk to be managed systematically across enterprises of all sizes. It includes comprehensive implementation guidelines, which explain how to gain support for the approach and get it up and running. The Information Risk Scorecard is an integral part of *FIRM*. The *Scorecard* is a form used to collect a range of important details about a particular information resource such as the name of the owner, criticality, level of threat, business impact and vulnerability.

The *ISF's* Information Security Status Survey (the Survey) is a comprehensive Risk Management tool that evaluates a wide range of security controls used by organizations to control the business risks associated with their IT-based information systems.

SARA is a detailed methodology for analyzing information risk in critical information systems. It consists of 4 phases:

- Planning
- Identify Business Requirements for Security
- Assess Vulnerability and Control Requirements
- Report

SPRINT is a relatively quick and easy-to-use methodology for assessing business impact and for analyzing information risk in important but not critical information systems. The full *SPRINT* methodology is intended to be applied to important, but not critical, systems. It complements the Forum's *SARA* methodology, which is better suited to analyzing the risks associated with critical business systems.

SPRINT first helps decide the level of risk associated with a system. After the risks are fully understood, *SPRINT* helps determine how to proceed and, if the *SPRINT* process continues, culminates in the production of an agreed plan of action for keeping risks within acceptable limits. *SPRINT* can help:

- identify the vulnerabilities of existing systems and the safeguards needed to protect against them;
- define the security requirements for systems under development and the controls needed to satisfy them.

A detailed description of ISF methods can be found in the annex III (s. chapter 17)

10.6 ISO/IEC IS 13335-2 (ISO/IEC IS 27005)

ISO/IEC IS 13335-2 is an *ISO* standard describing the complete process of information security Risk Management in a generic manner. The annexes contain examples of information security Risk Assessment approaches as well as lists of possible threats, vulnerabilities and security controls. *ISO/IEC IS 13335-2* can be viewed at as the basic information Risk Management standard at international level, setting a framework for the definition of the Risk Management process.

A detailed description of ISO/IEC IS 13335-2 can be found in the annex III (s. chapter 18)

10.7 ISO/IEC IS 17799:2005

This standard is of UK origin, but adapted to the international needs via *ISO*. This document shows what should be good practices in information processing. It is neither a method for evaluation nor for management of risks although a generic chapter refers to this issue. The document enlists various points that have to be taken into account to manage an information system suitably, even if some are not applicable within a specific company.

A detailed description of ISO/IEC IS 17799:2005 can be found in the annex III (s. chapter 19)

10.8 ISO/IEC IS 27001 (BS7799-2:2002)

This standard is dedicated to a process of certification. It enables the comparison of an information security management system through a series of controls. This standard does not cover risk analysis or certification of the Risk Management. Of UK origin, this standard has been adopted by *ISO* with some modifications. A certificate granted according to this standard confirms the compliance of an organization with defined requirements to information security management and a set of security controls.

A detailed description of ISO/IEC IS 27001 (BS7799-2:2002) can be found in the annex III (s. chapter 20)

10.9 IT-Grundschutz (IT Baseline Protection Manual)

IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain. The IT security process suggested by IT-Grundschutz consists of the following steps:

- Initialization of the process:
    - Definition of IT security goals and business environment
    - Establishment of an organizational structure for IT security

    - Provision of necessary resources

- Creation of the IT Security Concept:
    - IT-Structure Analysis
    - Assessment of protection requirements
    - Modeling
    - IT Security Check
    - Supplementary Security Analysis

- Implementation planning and fulfillment
- Maintenance, monitoring and improvement of the process
- IT-Grundschutz Certification (optional)

The key approach in *IT-Grundschutz* is to provide a framework for IT security management, offering information for commonly used IT components (modules). *IT-Grundschutz* modules include lists of relevant threats and required countermeasures in a relatively technical level. These elements can be expanded, complemented or adapted to the needs of an organization.

A detailed description of IT-Grundschutz can be found in the annex III (s. chapter 21)

10.10 MARION

The method *MARION* (Methodology of Analysis of Computer Risks Directed by Levels) arises from the *CLUSIF* (http://www.clusif.asso.fr/) and the last update was performed in 1998. It is based on a methodology of audit, which, as its name indicates, allows for estimating the level of IT security risks of a company through balanced questionnaires giving indicators in the form of notes on various subjects relative to security. The objective of the method is to obtain a vision of the company with regard to a level considered "correct", and on the other hand with regard to companies having already answered the same questionnaire. The level of security is estimated according to 27 indicators distributed in 6 large subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to ensure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is carried out to identify the risks (threats and vulnerabilities) that face the company.

Note: The *CLUSIF* does not sponsor this method anymore, as *MARION* is replaced by *MEHARI*. However, *MARION* is still used by various companies.

A detailed description of MARION can be found in the annex III (s. chapter 22)

10.11 MEHARI

MEHARI is a risk analysis method, designed by security experts of the *CLUSIF*. It proposes an approach for defining risk reduction measures suited to the organization objectives. *MEHARI* provides:

- a Risk Assessment model,
- modular components and processes.

MEHARI enhances the ability to:

- discover vulnerabilities through audit,
- analyze risk situations.

MEHARI includes formulas facilitating:

- threat identification and threat characterization,
- optimal selection of corrective actions.

A detailed description of MEHARI can be found in the annex III (s. chapter 23)

10.12 Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses)

The *Operationally Critical Threat, Asset, and Vulnerability Evaluation*^{SM} (*OCTAVE*®) approach defines a risk-based strategic assessment and planning technique for security. *OCTAVE* is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. *OCTAVE-S* is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). *OCTAVE-S* is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct *OCTAVE-S* effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

A detailed description of Octave v2.0 can be found in the annex III (s. chapter 24)

10.13 SP800-30 (NIST)

This product is one of the *Special Publication 800-series reports*. It gives very detailed guidance and identification of what should be considered within a Risk Management and Risk Assessment in computer security. There are some detailed checklists, graphics (including flowchart) and mathematical formulas, as well as references that are mainly based on US regulatory issues.

A detailed description of SP800-30 (NIST) can be found in the annex III (s. chapter 25)

10.14 Synthetic view on assessed methods

In this section a comparison at a glance of the methods assessed within the present inventory is presented. It should be noted that this table is based on a selected number of attribute values of the corresponding templates used for the description of methods (s. annex II on page 59). These attributes have been considered to be the most representative for a short comparison.

A fully fledged comparison of both methods and tools based on all attributes will be implemented in the electronic version of this document to be released in form of a Web Site.

Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (Information assessed in June 2006)	Size of organization	Skills needed[8]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	●●	●	●	●●●	●●●	●●●	●●●	DE	Free	All	**	N	N	Prototype (free of charge)
Cramm	●●●	●●●	●●●					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	●●●	●●●	●●●					NL	Free	All	*	N	N	
Ebios	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN, FR, DE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	●●	●●	●●	●●	●●●	●●●	●●●	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	●				●			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001					●	●		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	●●●	●●●	●●●					EN, FR	Not free	Large	*	N	N	

[8] Average skill level (see also attribute C1): * means basic level, ** means standard level, *** means specialist level.

Mehari	●●●	●●●	●●●					EN, FR	€100-500	All	**	N	N	RISICARE
Octave	●●	●●	●●	●●	●●	●●	●●	EN	Free	SME	**	N	N	
SP800-30 (NIST)	●●●	●●●		●●●	●●●	●●●		EN	Free	All	**	N	N	

Table 1: Comparison of the assessed Risk Management/Risk Assessment methods at a glance

The number of bullets (●, ●●, ●●●) used in these attributes varies from none to 3. It specifies the degree of fulfillment of the phase by the considered methods.

11 Inventory of Risk Management / Risk Assessment tools

ENISA has generated an inventory of Risk Management / Risk Assessment tools. A total of 12 tools have been considered. Similarly to the inventory of methods, each tool in the inventory has been described through a template. The template used consists of 22 attributes that describe characteristics of tools. The structure of the template and the meaning of each attribute can be found in annex V (s. annex V on page 116).

It is worth noting, that the inventory is not exhaustive. Tools included in the inventory have been chosen on the basis of their popularity. As the inventory is an **open** list, additional tools can be included in the future. For this purpose, ENISA is currently developing a process for submission of additional tools through vendors, as well as a process to update existing inventory entries.

The information included in this inventory has been assessed by ENISA by contacting the particular tool vendors. The assessment took place between December 2005 and March 2006 and reflects the development status of tools at that time. In cases of newer releases it might be the case that some of the tool properties described in the templates do not correspond to the current version. Through recurring assessments this information will be permanently updated.

In this chapter list the considered Risk Management / Risk Assessment tools are listed in short. For this purpose the text of the template attribute “description” has been included. For each tool a reference to its corresponding template in annex V is given.

11.1 Callio

Callio Secura 17799 is a product from *Callio technologies*. It is a web based tool with database support that let the user implement and certify an information security management system (ISMS). It supports the ISO17799 and ISO 27001 (BS 7799-2) standards and can produce the documents that are needed for certification. Moreover it provides document Management functionality as well as customization of tool’s databases. A trial version is available for evaluation.

A detailed description of Callio can be found in the annex V (s. chapter 26)

11.2 Casis:

CASIS software is an "Advanced Security Audit Trail Analyzer", meaning that its purpose is the collection of log file data across multiple systems, correlation of these data and production of security alerts based on user defined rules. The user is able to define new sources of data as well as to specify the alert output. *CASIS* is a product of *Aprico Consultants*.

A detailed description of Cobra can be found in the annex V (s. chapter 27)

11.3 Cobra:

Cobra is a stand-alone application for Risk Management from *C&A Systems Security*. It can be used for identification of threads and vulnerabilities and produces the appropriate countermeasures. The tool also provides ISO17799 compliance check. The tool is equipped with general knowledge databases (that are fully configurable) and moreover an e-Security knowledge base is provided. An evaluation copy is available from the web site of the product.

A detailed description of Cobra can be found in the annex V (s. chapter 28)

11.4 CounterMeasures:

Allion's product *CounterMeasures* performs Risk Management based on the US-NIST 800 series and OMB Circular A-130 USA standards. The user standardizes the evaluation criteria and using a "tailor-made" assessment checklist, the software provides objective evaluation criteria for determining security posture and/or compliance. *CounterMeasures* is available in both networked and desktop configurations and can be evaluated through a flash demonstration and a trial version.

A detailed description of Cobra can be found in the annex V (s. chapter 29)

11.5 Cramm:

The *Cramm tool* provides an easy way to implement the *Cramm method*, developed by *Insight Consulting*. All three stages of the method are fully supported using a staged and disciplined approach. The tool comes in three versions: CRAMM expert, CRAMM express and BS 7799 Review. A trial version is available for evaluation.

A detailed description of Cobra can be found in the annex V (s. chapter 30)

11.6 Ebios:

Ebios is a software tool developed by *Central Information Systems Security Division (France)* in order to support the *Ebios method.* The tool helps the user to produce all risk analysis and management steps according the five EBIOS phases method and allows all the study results to be recorded and the required summary documents to be produced. The *Ebios tool* is open source and free.

A detailed description of Cobra can be found in the annex V (s. chapter 31)

11.7 GStool:

GStool has been developed by *Federal Office for Information Security (BSI)* in order to support users of the IT Baseline Protection Manual. After collecting the information required, the users have a comprehensive reporting system at their disposal for carrying out structure analyses on all of their compiled data and for generating reports on paper or in electronic form. *GSTOOL* is a stand-alone application with database support. A trial version is available.

A detailed description of Cobra can be found in the annex V (s. chapter 32)

11.8 Isamm:

Isamm is a Risk Management tool from *Telindus*. It calculates an ideal security remediation plan containing all relevant actions sorted on the basis of their ROSI (Return on Security Investment). ISAMM Risk Assessments are today proposed as consultancy services and guided assessments. A tool has been developed for internal use by *Telindus* consultants.

A detailed description of Cobra can be found in the annex V (s. chapter 33)

11.9 Octave:

Octave Automated Tool has been implemented by *Advanced Technology Institute (ATI)* to help users with the implementation of the Octave and Octave-S approach. The tool assists the user during the data collection phase, organizes collected information and finally produces the study reports. A demonstration as well as a trial version is available for evaluation.

A detailed description of Cobra can be found in the annex V (s. chapter 34)

11.10 Proteus:

Proteus Enterprise is a product suite from *Infogov*. Through its components the user can perform gap analysis against standards such as ISO 17799 or create and manage an ISMS according to ISO 27001 (BS 7799-2). The tool is web-based with database support and may be evaluated though a trial version.

A detailed description of Cobra can be found in the annex V (s. chapter 35)

11.11 Ra2:

RA2 art of risk is a stand-alone tool from *AEXIS* for Risk Management based on the ISO 17799 and ISO 27001 standards. For each of the steps in this process the tool contains a dedicated step with report generation and printing out of the results. *RA2 Information Collection Device,* a component that is distributed along with the tool, can be installed

anywhere in the organization as needed to collect and feed back information into the Risk Assessment process. *AEXIS* provides a trial version of the tool.

A detailed description of Cobra can be found in the annex V (s. chapter 36)

11.12 RiskWatch:

RiskWatch for Information Systems & ISO 17799 is the of RiskWatch company' solution for IS Risk Management. This tool conducts automated risk analysis and vulnerability assessments of information systems. The knowledge databases that are provided along with the product are completely customizable by the user, including the ability to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. The tool includes controls from the ISO 17799 and US-NIST 800-26 standards. RiskWatch provides an online demonstration of this product.

A detailed description of Cobra can be found in the annex V (s. chapter 37)

12 Open issues – Road map for further activities in Risk Management

After discussions with various experts in the relevant field (e.g. experts of the Working Group on Risk Management / Risk Assessment, other external experts) and evaluation of relevant literature [RM-Article], [ISO 13335-2], [Ricciuto], some open problems and needs in the area of Risk Management have been identified:

1. *Need to enhance* ***comparability/interoperability of methods and tools*** *(e.g. by improving description in the inventories)*: Additional characteristics of methods and tools that will enable a more exhaustive comparison have to be introduced. Such characteristics concern detailed properties of methods and tools that are hidden in the supported functionality (e.g. kind and quality of security measurements, kind and quality of threats, number of existing good practices based on those methods and tools etc.). Further, the interoperability of methods and tools will allow the comparison of assessments and the risk level of particular applications assessed via those. Finally a procedure for the future maintenance of the established inventories is necessary in order to keep them accurate.

2. *Need to* ***identify combinations of methods*** *to fulfill organizational requirements*: based on the above, there is a need to elaborate on possible used combinations of methods and tools that are best suited for use within a sector (e.g. telecommunications, finance, commerce etc.). Combination of methods and tools are used in order to fill gaps and weaknesses inherent to native Risk Management/Risk Assessment methods and tools.

3. *Need to* ***generate demonstrators and awareness material*** *for the use of methods*: examples about the usage of the assessed methods and tools have to be developed. Such examples have to anticipate the entire life-cycle of Risk Management while considering common application scenarios found in variety of organizations (e.g. Risk Management for open interconnected systems, risks of networked components etc.).

4. *Consideration of* ***continuity and emerging risks***: both continuity and emerging risks hold an important position within IT risks. As mentioned in the ENISA regulation but also in relevant sources (e.g. daily news, regulation about critical infrastructures, forums etc.), continuity of IT operations is one of the key success elements of today's companies. Similarly, the identification of new risks emerging through new technologies is key objective of information society.

5. ***Generation of an installed software*** *base of tools, methods and applications; and performance of risk assessments for applications*: to enhance hands-on experience at ENISA, a number of software tools on Risk Management and Risk Assessment will be installed. This is a precondition for point 3 above. Furthermore, this will enable ENISA to perform on demand assessments of strategic application areas

and services (e.g. mobile systems, applications in the area of ambient intelligence, VoIP, etc). Experience shows that in such application areas Risk Assessments – if any - are always performed ex-post (with all related problems emanating from such approaches).

6. *Need for examples depicting the* ***integration of Risk Management with other processes/disciplines***: integration of Risk Management/Risk assessment to operational processes of organizations is a key issue for successful implementation. Integration examples with de-facto standards in this area (e.g. ITIL [ITIL]) will enhance the successful usage of Risk Management/Risk Assessment.

The problems and needs identified are addressed in detail in the subsections of this chapter. Besides the set of actions to address them, drivers to help readers better understand the importance of the identified activities are also given. Some of the detailed points of each activity have been formulated as questions in order to underline the related problems.

The priority of the identified problems and needs is expressed by means of a generic time window divided into short, medium and long term periods of action. A short term period of action is assumed to be 1 year, a medium term is1-2 years and long term 2-3 years. The shorter its term, the higher the priority assigned to a certain open issue and its corresponding activities (s. section 12.7).

12.1 Comparability/interoperability of methods and tools

- **Activity 1: Establish 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.

- **Activity 2: Compatibility/interoperability of methods**
  This activity embraces several issues concerning comparability and interoperability of methods (and tools):

  - 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 increasingly common practice. Similar activity has already been identified (but not yet solved) by experts in the relevant field (e.g. EBIOS club).

- **Activity 3: Measurements of risks**
  What (types of) qualitative methods do exist?
  What (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.

- **Activity 4: Method and tool inventory maintenance**
  What are the functions needed to maintain an inventory? (Enter, remove or update methods and tools).

  What is the minimum 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 for to the inputs to the above points?

  Driver: New methods / tools are constantly being developed. Existing ones are constantly maintained. As ENISA inventories are open lists, 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).

12.2 Identification of combinations of methods

- **Activity 1: Merging of methods**

One organization 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 increasingly relevant ([ENISA-BSI WS]).

12.3 Generation of demonstrators and awareness material

- **Activity 1: 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?

  The above questions pinpoint the need for training and awareness material for a wide variety of users (from expert and novice users). Whether the demonstrators mentioned above will have to be grouped to form training units on various aspects of Risk Management and Risk Assessment will be taken under consideration.

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

12.4 Continuity and Emerging Risks

- **Activity 1: 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?

  Answers to the above questions, will enable initial coverage of availability risks at a satisfactory degree of penetration (s. also Figure 5 in annex VI).

  Driver: Business Continuity Planning is an integral part of Risk Management when facing continuity and availability risks.

- **Activity 2: Emerging risks**
  Emerging risks cope with the identification of risks that might emerge through the use of future applications. As such, Emerging Risks are not based on experience but rather on prediction. To this extend, the generation of good usage and

technology scenarios is decisive for the successful prediction of Emerging Risks. Accordingly, in order to elaborate on this area, questions like the ones bellow are fundamental:

Are there existing methods to identify emerging risks (which)?
Are there any suggestions for methods concentrating in emerging risks?
What are possible threat agents (current and future)?
Are there any examples of emerging risk scenarios?
What are those relevant factors ones should examine and take into account in order to prevent emerging risk realization?
Are there any action points one should investigate in order to plan its emerging risk related actions?
Are there any models to specify dependability (assets, threats, and attack scenarios)?
Are there any suggestions to gather, handle and disseminate information regarding emerging risks both internally and externally within different timeframes?

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

12.5 Generation of an installed software base

- **Activity 1: Installation of tools and evaluation of applications**
  It is common that new application areas are initially developed without systematic anticipation of security (e.g. confidentiality, privacy, anonymity etc.). Particular applications such as ambient intelligence, e-Health applications, mobile protocols, and Identity Management are some examples. This is often tied to the fact that in initial design phases neither relevant security know-how nor specified responsibilities have been defined as part of the project (e.g. because of shortage of monetary or know-how resources).

  Driver: ENISA Stakeholders have often expressed their interest in having ENISA as a contributor to security issues of applications and systems. Risk Assessments is one major activity in determining security properties of applications.

12.6 Integration of Risk Management with other processes/disciplines

- **Activity 1: Risk Management interfaces with other processes**
  The interfaces of Risk Management with other relevant security and operational 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
- Risk Management and operational processes (e.g. ITIL [ITIL])

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.).

12.7 Priorities

In this section priorities to the identified open issues and their activities have been assigned. The priorities assigned to issues and activities are represented below in concise form by means of a table.

Compatibility/interoperability of methods and tools		
Activity	**Priority**	**Comment**
Activity 1: Establish unified information bases for Risk Management	↑ Short term (high priority)	This activity has been included in the Terms of Reference for the ENISA ad hoc Working Group on Risk Management/Risk Assessment for 2006-2007
Activity 2: Compatibility/ interoperability of methods	↑ Short term (high priority)	
Activity 3: Measurements of risks	↑ Short term (high priority)	
Activity 4: Method and tool inventory maintenance	↑ Short term (high priority)	This activity has been included in the Terms of Reference for the ENISA ad hoc Working Group on Risk Management/Risk Assessment 2006-2007
Identification of method combinations		
Activity	**Priority**	**Comment**
Activity 1: Merging of methods	↑ Short term (high priority)	
Generation of demonstrators and awareness material		
Activity	**Priority**	**Comment**
Activity 1: Awareness, training, communication	↑ Short term (high priority)	
Continuity and Emerging Risks		
Activity	**Priority**	**Comment**
Activity 1: Business Continuity Planning	↗ Short to medium term (high/medium priority)	
Activity 2: Emerging Risks	↑ Short term (high priority)	This activity has been addressed in the ENISA Work Programme 2006.

Generation of an installed software base		
Activity	**Priority**	**Comment**
Activity 1: Installation of tools and evaluation of applications	↗ Short to medium term (high/medium priority)	This activity will be partially implemented within the ENISA Technical Cabinet (to be initiated in 2006)
Integration of Risk Management with other processes/disciplines		
Activity	**Priority**	**Comment**
Activity 1: Risk Management interfaces with other processes	↗ Short to medium term (high/medium priority)	

Table 2: Priorities of open issues and their activities

In the coming years, ENISA may bring important contributions to these priorities, both through the successive yearly Work Programmes and possible requests received from important national and European bodies.

Bibliography

BASEL II	Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, May 2001 www.bis.org
CC	ISO/IEC 15408-1:2005, Information technology -- Security techniques -- Evaluation criteria for IT security www.iso.ch
Cobit	CobiT, Control Objectives for Information and related Technology, IT Governance Institute www.isaca.org
EBIOS	Expression of Needs and Identification of Security Objectives PREMIER MINISTRE Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil www.ssi.gouv.fr
Emerging Risk ENISA	ENISA Study on Emerging Risks: Security and Privacy Risks in Future IT (provisional title), ENISA, to appear in 2006
Emerging Risk IPTS	Final Report – Future Threats and Crimes In An Ambient Intelligent Everyday Environment, Dr J R Walton, 2005, supplied by QinetiQ and Transcrime for JRC / IPTS www.jrc.es
ENISA Regulation	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 www.enisa.eu.int
ENISA-BSI WS	"ENISA-BSI Information Security Management Days", Bonn, Germany 10/11/2005
ENISA-WG	ENISA ad hoc Working Group on technical and policy aspects of Risk Assessment and Risk Management, June 2005 – March 2006 http://www.enisa.eu.int/doc/pdf/ad_hoc_wg/Group_Members_rarm.pdf

Guide 73	ISO/IEC Guide 73:2002, Risk management -- Vocabulary -- Guidelines for use in standards www.iso.ch
HAZOP	Neil Storey: Safety-critical computer systems; Addison-Wesley, 1996
ISO 13335-2	ISO/IEC TR 13335-2:1997, Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security www.iso.ch
ISO 17799	ISO/IEC 17799:2005, Information technology -- Security techniques -- Code of practice for information security management www.iso.ch
IT-Grund	BSI-Standard 100-1, 100-2, 100-3 BSI-Empfehlungen des zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit www.bsi.de
ITIL	IT Infrastructure Library, OGC – Office of Government Commerce, also released as: ISO/IEC 20000:2005, Information technology -- Service management www.iso.ch
ITSEC	Information Technology Security Evaluation Criteria (ITSEC), Luxembourg: Office for Official Publications of the European Communities, 1991, http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf
NIST	G. Stonebumer, A. Goguen, A Fringa, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, July 2002
OCTAVE	OCTAVE Method Implementation Guide Version 2.0, Carnegie Mellon University, June 2001 www.cert.org/octave
Ricchiuto	Arcangelo Ricchiuto, Diploma work: “ITIL and Risk Management process integration”, University of Applied Sciences Cologne, July 2005 (available in German)

RM-Article	Colin Dixon, CWSECURITY PROFESSIONALS, User Groups, How information risk management underpins good corporate governance, Monday 1st August 2005
SIZ-DE	SIZ Sicherer IT- Betrieb, Framework for security of the German Savings Banks Organization, 2006 http://www.siz.de/siz-produkte/sicherheitstechnologie/sicherer_it-betrieb/index.htm
SIZ-PP	Schutzprofil SIZ-PP, Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, SIZ-GbmH, Bonn, 1998/99/2000
SOX	Sarbanes-Oxley Act of 2002, H.R. 3763, An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes, 23 January 2002
WG-Deliverable 1	ENISA ad hoc working group on risk assessment and risk management, Inventory of risk assessment and risk management methods, Deliverable 1, Final version, Version 1.0, 2006
WG-Deliverable 2	ENISA ad hoc working group on risk assessment and risk management, Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs) Deliverable 2, Final version, Version 1.0, 2006
WG-Deliverable 3	ENISA ad hoc working group on risk assessment and risk management, Road map, Deliverable 3, Final version, Version 1.0, 2006

ANNEX I: Glossary

G.1	**Acceptable Risk**	The level of **residual risk** (G.26) that has been determined to be a reasonable level of potential loss/disruption for a specific system. *(CIAO – Critical Infrastructure Assurance Office - U.S.A)*
G.2	**Accountability**	The property that ensures that the actions of an entity may be traced uniquely to the entity. *(ISO/IEC PDTR 13335-1)* • This may cover non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. *(ENISA)*
G.3	**Asset**	Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.. *(ISO/IEC PDTR 13335-1)*
G.4	**Consequence**	Outcome of an **event** (G.11) • There can be more than one consequence from one event. • Consequences can range from positive to negative. • Consequences can be expressed qualitatively or quantitatively *(ISO/IEC Guide 73)*
G.5	**Contingency Plan**	A plan for emergency response, backup operations, and post-disaster recovery in a system, as part of a security program, to ensure availability of critical system resources and facilitate continuity of operations in a crisis. *(ENISA)*
G.6	**Data Availability**	The fact that data is accessible and services are operational. *(ENISA)*
G.7	**Data Confidentiality**	The protection of communications or stored data against interception and reading by unauthorized persons. *(ENISA)* The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. *(ISO/IEC PDTR 13335-1)*
G.8	**Data Integrity**	The confirmation that data which has been sent, received, or stored are complete and unchanged. *(ENISA)* The property that data has not been altered or destroyed in an unauthorized manner. *(ISO/IEC PDTR 13335-1)*
G.9	**Definition of Scope**	Process for the establishment of global parameters for the performance of Risk Management within an organization. Within the definition of scope for Risk Management internal

and external factors have to be taken into account.
(ENISA)

G.10 Disaster Recovery

The process of restoring a system to full operation after an interruption in service, including equipment repair / replacement, file recovery / restoration.
(ENISA)

G.11 Event

Occurrence of a particular set of circumstances

- The event can be certain or uncertain.
- The event can be a single occurrence or a series of occurrences.

(ISO/IEC Guide 73)

G.12 Evidence

Information that either by itself or when used in conjunction with other information is used to establish proof about an **event** (G.11) or action.

- Evidence does not necessarily prove truth or existence of something but contributes to establish proof.

(ENISA)

G.13 Exposure

The potential loss to an area due to the occurrence of an adverse **event** (G.11). *(ISACA)*

- Generally, in the **Risk Management** (G.39) **process** (G.24) a risk does not always represent a loss or a negative consequence but can also be an opportunity or a result of a positive event.
  (ENISA)

G.14 Gap Analysis

A comparison that identifies the difference between the actual and the expected / specified system status.
(ENISA)

G.15 Impact

The result of an unwanted **incident** (G.17).
(ISO/IEC PDTR 13335-1)

G.16 Impact Analysis

The identification of critical business **processes** (G.24), and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes.

- Business impact analysis identifies:
  - the form the loss or damage will take
  - how that degree of damage or loss is likely to escalate with time following an incident
  - the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level
  - the time for full recovery of the business processes

(ENISA)

G.17 Incident

An **event** (G.11) that has been assessed as having an actual or potentially adverse effect on the security or performance of a

		system. *(ENISA)*
G.18	**Interested Party**	Person or group having an interest in the performance or success of an organization's mission or objectives. *(ISO/IEC Guide 73)*
G.19	**Mitigation**	Limitation of any negative **consequence** (G.4) of a particular **event** (G.11). *(ISO/IEC Guide 73)*
G.20	**Monitor and Review**	A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions. *(ENISA)*
G.21	**Priority**	Sequence in which an **incident** (G.17) or problem needs to be resolved, based on **impact** (G.15) and urgency. *(ENISA)*
G.22	**Probability**	Extent to which an **event** (G.11) is likely to occur. *(ENISA)*
G.23	**Procedure**	A written description of a course of action to be taken to perform a given task. *(ENISA)*
G.24	**Process**	An organized set of activities which uses resources to transform inputs to outputs. *(ENISA)*
G.25	**Process Owner**	An individual held accountable and responsible for the workings and improvement of one of the organization's defined **processes** (G.24) and its related sub-processes. *(ENISA)*
G.26	**Residual Risk**	**Risk** (G.27) remaining after **risk treatment** (G.45). *(ISO/IEC Guide 73)*
G.27	**Risk**	The potential that a given threat will exploit vulnerabilities of an **asset** (G.3) or group of assets and thereby cause harm to the organization. (ISO/IEC PDTR 13335-1)
G.28	**Risk Acceptance**	Decision to accept a **risk** (G.27) by the responsible management of the organization. • Risk acceptance depends on risk criteria defined within the process **Definition of Scope** (G. 9). *(Definition adopted from ISO/IEC Guide 73 with some*

modification by ENISA)

G.29 Risk Analysis

Systematic use of information to identify **sources** (G.48) and to estimate the **risk** (G.27)

- Risk analysis provides a basis for **risk evaluation** (G.36), **risk treatment** (G.45) and **risk acceptance** (G.28).

(ISO/IEC Guide 73)

G.30 Risk Assessment

A scientific and technologically based **process** (G.24) consisting of three steps, **risk identification** (G.38), **risk analysis** (G.29) and **risk evaluation** (G.36).
(ENISA)

G.31 Risk Avoidance

Decision not to become involved in, or action to withdraw from, a **risk** (G.27) situation.
(ISO/IEC Guide 73)

G.32 Risk Communication

A **process** (G.24) to exchange or share information about **risk** (G.27) between the decision-maker and other **stakeholders** (G.50).

- The information can relate to the existence, nature, form, **probability** (G.22), severity, acceptability, treatment or other aspects of risk.

(ISO/IEC Guide 73)

G.33 Risk Control

Actions implementing **risk management** (G.39) decisions.

- **Risk** (G.27) control may involve monitoring, re-evaluation, and compliance with decisions.

(ISO/IEC Guide 73)

G.34 Risk Criteria

Terms of reference by which the significance or **risk** (G.27) is assessed.

- Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic aspects, the concerns of **stakeholders** (G.50), **priorities** (G.21) and other inputs to the assessment.

(ISO/IEC Guide 73)

G.35 Risk Estimation

Process (G.24) used to assign values to the **probability** (G.22) and **consequences** (G.4) of a **risk** (G.27).

- It can consider cost, benefits, the concerns of **stakeholders** (G.50) and other variables, as appropriate for **risk evaluation** (G.36).

(ISO/IEC Guide 73)

G.36 Risk Evaluation

Process (G.24) of comparing the estimated **risk** (G.27) against given **risk criteria** (G.34) to determine the significance of risk.

(ISO/IEC Guide 73)

G.37 Risk Financing

Provision of funds to meet the cost of implementing **risk treatment** (G.45) and related costs.
(ISO/IEC Guide 73)

G.38 Risk Identification

Process (G.24) to find, list and characterize elements of **risk** (G.27).
(ISO/IEC Guide 73)

G.39 Risk Management

The **process** (G.24), distinct from **risk assessment** (G.30), of weighing policy alternatives in consultation with **interested parties** (G.18), considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.
(ENISA)

G.40 Risk Optimization

Process (G.24), related to a **risk** (G.27) to minimize the negative and to maximize the positive **consequences** (G.4) and their respective **probabilities** (G.22).

- Risk optimization depends upon **risk criteria** (G.34), including costs and legal requirements.

(ISO/IEC Guide 73)

G.41 Risk Perception

Way in which a **stakeholder** (G.50) views a **risk** (G.27), based on a set of values or concerns.

- Risk perception depends on the stakeholder's needs, issues and knowledge.
- Risk perception can differ from objective data.

(ISO/IEC Guide 73)

G.42 Risk Reduction

Actions taken to lessen the **probability** (G.22), negative **consequences** (G.4) or both, associated with a **risk** (G.27).
(ISO/IEC Guide 73)

G.43 Risk Retention

Acceptance of the burden of loss, or benefit of gain, from a particular **risk** (G.27).

- Risk retention includes the acceptance of risks that have not been identified.
- Risk retention does not include treatments involving insurance, or transfer by other means.

(ISO/IEC Guide 73)

G.44 Risk Transfer

Sharing with another party the burden of loss or benefit of gain, for a **risk** (G.27).

- Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk.
- Risk transfer can be carried out through insurance or other

agreements.
- Risk transfer can create new risks or modify existing risk.

(ISO/IEC Guide 73)

G.45 Risk Treatment

Process (G.24) of selection and implementation of measures to modify **risk** (G.27).

- Risk treatment measures can include avoiding, optimizing, transferring or retaining risk

(ISO/IEC Guide 73)

G.46 Safeguards

Practices, **procedures** (G.23) or mechanisms that reduce **risk**.

- The term 'safeguard' is normally considered to be synonymous with the term 'control'**.**

(ISO/IEC PDTR 13335-1)

G.47 Security

All aspects related to defining, achieving, and maintaining data **confidentiality** (G.7), **integrity** (G.8), **availability** (G.6), **accountability** (G.2), authenticity, and reliability.
- A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way.

(ISO/IEC WD 15443-1)

G.48 Source

Item or activity having a potential for a **consequence** (G.4)
(ISO/IEC Guide 73)

G.49 Source Identification

Process (G.24) to find, list and characterize **sources** (G.48)
(ISO/IEC Guide 73)

G.50 Stakeholder

Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, a **risk** (G.27).
(ISO/IEC Guide 73)

G.51 Threat

Any circumstance or event with the potential to adversely impact an **asset** (G.3) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
(ENISA)

G.52 Vulnerability

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable **event** (G.11) compromising the security of the computer system, network, application, or protocol involved.
(ITSEC)

ANNEX II: Structure of template for method description

The ENISA Working Group has defined attributes in order to classify methods and in particular their level of visibility in the market and their main features and functions.

These attributes are categorized as follows:

A: "***Product Identity card***",
B: "***Product Scope***" and
C: "***Users viewpoint***".

Both attribute categories and attribute semantics are presented in the forthcoming sections.

A: Product Identity card

1: General information

This attribute holds basic information to identify the product. The information provided here contains the name of the product, the company or cross-frontier organization that provides the product and the country of origin (in case the product originated from a company or national organization).

2: Level of reference of the product

Details about the type of initiator of the product like:

- National Standardization body
- International Standardization body
- Private sector organization / association
- Public / government organization

3: Identification

Method: primarily a set of consistent documents, stating how to conduct Risk Assessment (RA) or Risk Management (RM) and not requiring an installation of an application on a computer.
When standard: specify if issued by a national or international body[9].
A brief description of the product is given.

The number of bullets used in these attributes varies from none to 3. It specifies the degree of fulfillment of the phase by the considered product.

4: Lifecycle

Date of the first edition, as well as date and number of actual version.

[9] Some redundancy among the content of attributes has intentionally been kept in order to enhance comprehensiveness.

5: Useful links

Official web site: hyperlink to the site of the originator/provider of the product, where to download the product or order it.
Related user group web site: hyperlink to the web site of the user group (if any) for the product.
Main relevant web site: web site that offers relevant and neutral information concerning the product.

6: Languages

Languages available: the first occurrence gives the language that was used to develop the product. Other occurrences are languages in which the product is available within the European Union.

7: Price

Free: the solution is free of charge.
Not free: the price to buy or the yearly fee (this also includes membership fees to acquire access to the product, e.g. ISO standards).
Updating fee: the yearly fee for updates.

B: Scope

1: Target organizations

Defines the most appropriate type of organizations the product aims at:

- **Governments, agencies**: the product is developed by organizations working for a state (e.g. a national information security authority).
- **Large companies**: the product is useful for companies with more than 250 employees.
- **SME**: the product is useful for small and medium size companies that cannot afford dedicated Risk Management personnel or complete segregation of duties.
- **Commercial companies**: the product is targeted to companies that have to implement it due to commercial demands from stakeholders, financial regulators, etc.
- **Non-profit**: companies where commercial benefits are not essential like the NGO's health sector, public services, etc.
- **Specific sector**: the product is dedicated to a very specific sector (e.g. nuclear, transportation) and usually cannot be used in other sectors.

2: Geographical spread

Used in EU member states: list of EU member states in which implementation is known by working group members. This includes organization as:

- European institutions (e.g. European Commission, European Union Council, European agencies).

- International organizations located in Europe (e.g. NATO, UNO, OECD, UNESCO).

Used in non-EU countries: used within potential new member states of the European Union or outside the EU (e.g. Switzerland or USA).

3: Level of detail

The targeted kind of users is:

- Management level: generic guidelines.
- Operational level: guidelines for implementation planning with a low level of detail.
- Technical level: specific guidelines, concerning technical, organizational, physical and human aspects of IT Security with a high level of detail.

4: License and certification scheme

Recognized licensing scheme[10]: there is a recognized scheme for consultants/firms stating their mastering of a method.
Existing certification scheme: an organization may obtain a certificate, that it has fully and correctly implemented the method on its information systems.

C: Users viewpoint

1: Skills needed

Three types of skills are considered:

- **To introduce** (the skills needed to understand the dependencies among the specific details of the product, e.g. different concepts supported, phases, activities etc.)
- **To use** (the specific qualifications needed in order to perform current work, e.g. documentation easy to understand and use), and
- **To maintain** (the specific qualifications needed to maintain the life cycle of the product, e.g. to customize, tailor or perform regular updates)

For each type, the level of skills is classified according to the following scale:

- **Basic** level: common sense and experience.
- **Standard** level: some days or weeks of training are sufficient.
- **Specialist** level: thorough knowledge and experience is required.

2: Consultancy support

[10] License is used in that document to name the process of issuing to an individual a certificate by a certification body on his mastering of the method.

It is necessary to use external help (consultancy) in order to apply the product. In such cases, the product can be open to any consultant on the market or is it bound to a specific category of consultants (e.g. licensed).

3: Regulatory compliance
There is a given compliance of the product with international regulations (e.g. Basel II, Sarbanes Oxley Act).

4: Compliance to IT standards
There is a compliance with a national or international standard (e.g. ISO/IEC IS 13335-1, ISO/IEC IS 15408).

5: Trial before purchase
Details regarding the evaluation period (if any) before purchase of the product.

6: Maturity level of the Information system
The product gives a means of measurement for the maturity of the information system security (e.g. through a reasoned best practice document).

7: Tools associated with the product
List of tools that support the product (commercial tools as well as non-commercial ones). If relevant, the organizations/sectors that can obtain the tool for free are mentioned.

8: Technical integration of available tools
Particular supporting tools (see C-7) can be integrated with other tools (e.g. CERT tools).

9: Organizational integration
The method provides interfaces to existing processes within the organization (e.g. project management, procurement, etc.)

10: Flexible knowledge database
It is possible to adapt a knowledge database specific to the activity domain of the company.

ANNEX III: Inventory of methods

13 Austrian IT Security Handbook

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
Österreichisches IT-Sicherheitshandbuch (Austrian IT Security Handbook)	Bundeskanzleramt (Austrian federal chancellery)	Austria

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
			Austrian federal chancellery

3. Identification

R.A. Method	R.M. Method	National standard	International standard
	X		

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●	The handbook contains a generic description of RA, but does not specify a special method
Risk analysis	●	
Risk evaluation	●	

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●●	part 1, chapter 4
Risk treatment	●●●	part 1, chapter 5.1, part 2
Risk acceptance	●●●	part 1, chapter 5.2
Risk communication	●●●	part1, chapters 5.5 and 6.2

Brief description of the product:

The *Austrian IT Security Handbook* consists of 2 parts. Part 1 gives a detailed description of the IT security management process, including development of security policies, risk analysis, design of security concepts, implementation of the security plan and follow-up activities. Part

2 is a collection of 230 baseline security measures. A tool supporting the implementation is available as a prototype. The *Austrian IT Security Handbook* was originally developed for government organizations, and is now available for all types of business. The handbook is compliant with ISO/IEC IS 13335, the German IT-Grundschutzhandbuch and partly with ISO/IEC IS 17799.

4. Lifecycle

Date of the first release	Date and identification of the last version
1998	Version 2.2, November 2004

5. Useful links

Official web site	http://www.cio.gv.at/securenetworks/sihb/
User group web site	
Relevant web site	

6. Languages

Availability in European languages	DE

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	AT
Used in non-EU countries	

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Not necessary	

3. Regulatory compliance
NA

4. Compliance to IT standards

ISO/IEC IS 13335-1, -2	ISO/IEC IS 17799 (partly)

5. Trial before purchase

CD or download available	Identification required	Trial period
Product is free		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
Yes, in prototype status (free of charge)	

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Business continuity, change management, system management

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

14 Cramm

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
CRAMM (CCTA Risk Analysis and Management Method)	Insight Consulting	United Kingdom

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
			British CCTA (Central Communication and Telecommunication Agency)

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X			

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	In CRAMM tool
Risk analysis	●●●	In CRAMM tool
Risk evaluation	●●●	In CRAMM tool

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	-	
Risk treatment	-	
Risk acceptance	-	
Risk communication	-	

Brief description of the product:

CRAMM is a risk analysis method developed by the British government organization *CCTA* (Central Communication and Telecommunication Agency), now renamed zhe Office of Government Commerce (OGC). A tool having the same name supports the method: *CRAMM*. The *CRAMM* method is rather difficult to use without the *CRAMM* tool. The first releases of

CRAMM (method and tool) were based on best practices of British government organizations. At present *CRAMM* is the UK government's preferred risk analysis method, but *CRAMM* is also used in many countries outside the UK. *CRAMM* is especially appropriate for large organizations, like government bodies and industry.

4. Lifecycle

Date of the first release	Date and identification of the last version
1985	2003 (version 5)

5. Useful links

Official web site	http://www.cramm.com
User group web site	http://www.crammgebruiksgroep.nl (in Dutch)
Relevant web site:	www.insight.co.uk

6. Languages

Availability in European languages	EN, NL, CZ

7. Price

Free	Not free	Updating fee
	Unknown	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X			
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Specialist	Specialist	Specialist

2. Consultancy support

Open market	Company specific
Yes	

3. Regulatory compliance

GLBA	HIPPA

4. Compliance to IT standards

ISO/IEC IS 17799

5. Trial before purchase

CD or download available	Registration required	Trial period
	Yes	

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
	CRAMM expert (Insight), CRAMM express (Insight)

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

15 Dutch A&K analysis

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
Afhankelijkheids- en kwetsbaarheidsanalyse (A&K analysis)	Dutch ministry of internal affairs	The Netherlands

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
			Dutch ministry of internal affairs

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X			

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	Handbook, part 2+3
Risk analysis	●●●	Handbook, part 2+3
Risk evaluation	●●●	Handbook, part 2+3

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	-	
Risk treatment	-	
Risk acceptance	-	
Risk communication	-	

Brief description of the product:

The method *Afhankelijkheids- en Kwetsbaarheidsanalyse* (*A&K analysis*) was developed in draft form by the Dutch public company *RCC*. The Dutch ministry of internal affairs completed the development in 1996 and published a handbook describing the method. The method has not been updated since that time. The *A&K analysis* is the unique and preferred method for risk analysis by Dutch government bodies since 1994. Besides the Dutch government, Dutch companies often use *A&K analysis*.

4. Lifecycle

Date of the first release	Date and identification of the last version
About 1980	July, 1996, version 1.01

5. Useful links

Official web site	
User group web site	
Relevant web site	
Other relevant sources	Handbook: 'Handleiding Afhankelijkheids- en Kwetsbaarheidsanalyse: stappenplan voor de uitvoering van een A&K-analyse' (in Dutch), version 1.01, Ministry of Internal Affairs, The Hague, 1996, The Netherlands

6. Languages

Availability in European languages	NL

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	NL
Used in non-EU countries	

3. Level of detail

Management	X	Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain

Basic	Standard	Basic

2. Consultancy support

Open market	Company specific
Not necessary	

3. Regulatory compliance

VIR (Dutch Government Information Security Act)

4. Compliance to IT standards

ISO/IEC IS 17799

5. Trial before purchase

CD or download available	Registration required	Trial period
N.A.		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
	Several, but not certified

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

16 Ebios

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)	DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information, Premier Ministre)	France

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
		Club EBIOS, gathering about 60 enterprises, French ministries, and independent experts.	

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X		

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	Section 3, Step 3: study of threat sources, study of vulnerabilities, formalization of threats, and justification for discarding threats. Section 3, Step 4, Activity 4.1: risk opportunity, and its consequences (security needs, and impacts)
Risk analysis	●●●	Section 3, Step 3, Activity 3.1: security criteria affected by attack methods, type of threat agent, cause of threat agent, assessment of attack potential Section 3, Step 3, Activity 3.2: identification of vulnerabilities according to attack methods, assessment of vulnerability levels. Section 3, Step 3, Activity 3.3: explicit formulation of threat, assessment of threat opportunity.
Risk evaluation	●●●	Section 3, Step 3, Activity 3.3: threat opportunity Section 4, Step 4, Activity 4.1: risk formulation

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●●	Section 3, Step 1, Section 3, Step 2, Section 3, Step 3, Section 3, Step 4, Activity 4.1
Risk treatment	●●●	Section 3 Section 4, Steps 4.2, Section 4, Step 4.3, Section 5: The security objectives statement expresses the will to cover identified risks by security requirements. These requirements specify how to reach those objectives by security measures, e.g. by means of internal knowledge bases as well as of external ones such as IT-Grundschutz, or catalogues of best practices (ISO/IEC IS 17799, ISO/IEC IS 15408, etc…)
Risk acceptance	●●●	Section 2, Section 3 Step 4: Retained / non-retained risks, Security objectives statement, proof of retained risks coverage by objectives, highlighting of residual risks Section 3, Step 5: security requirements statement, proof of objectives coverage by requirements, highlighting of residual risks.
Risk communication	●●●	Section 1, Software that produces wide variety of deliverables in a standardized format Training

Brief description of the product:

EBIOS is a comprehensive set of guides (plus a free open source software tool) dedicated to Information System risk managers. Originally developed by the French government, it is now supported by a club of experts of diverse origin. This club is a forum on Risk Management, active in maintaining *EBIOS* guides. It produces best practices as well as application documents targeted to end-users in various contexts. *EBIOS* is widely used in the public as well as in the private sector, both in France and abroad. It is compliant with major IT security standards.

EBIOS gives risk managers a consistent and high-level approach to risks. It helps them acquire a global and coherent vision, useful for support decision-making by top managers on global projects (business continuity plan, security master plan, security policy), as well as on

more specific systems (electronic messaging, nomadic networks or web sites for instance). *EBIOS* clarifies the dialogue between the project owner and project manager on security issues. In this way, it contributes to relevant communication with security stakeholders and spreads security awareness.

EBIOS approach consists of a cycle of 5 phases:

- Phase 1 deals with context analysis in terms of global business process dependency on the information system (contribution to global stakes, accurate perimeter definition, relevant decomposition into information flows and functions).
- Both the security needs analysis and threat analysis are conducted in phases 2 and 3 in a strong dichotomy, yielding an objective vision of their conflicting nature.
- In phases 4 and 5, this conflict, once arbitrated through a traceable reasoning, yields an objective diagnostic on risks. The necessary and sufficient security objectives (and further security requirements) are then stated, proof of coverage is furnished, and residual risks made explicit.

EBIOS turns out to be a flexible tool. It may produce a wide range of deliverables (*SSRS*, security target, protection profile, action plan, etc). Local standard bases (e.g.: *German IT Grundschutz*) are easily added on to its internal knowledge bases (attack methods, entities, vulnerabilities) and catalogues of best practices (*EBIOS* best practices, *ISO/IEC IS 17799*).

4. Lifecycle

Date of the first release	Date and identification of the last version
Release 1 in 1995	Release 2 in June 2004

5. Useful links

Official web site	http://www.ssi.gouv.fr
User group web site	
Relevant web site	http://ebios.cases-cc.org

6. Languages

Availability in European languages	FR, EN, DE, ES

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X

Specific sector	

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	Yes
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
If support is needed, a wide variety of private consultants is available	

3. Regulatory compliance

NA

4. Compliance to IT standards

ISO/IEC IS 27001	ISO/IEC IS 15408	ISO/IEC IS 17799	ISO/IEC IS 13335	ISO/IEC IS 21827

5. Trial before purchase

CD or download available	Registration required	Trial period
Product is free		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	Yes, with compliance to ISO/IEC 21827. The document is available at: www.ssi.gouv.fr/fr/confiance/documents/Methodes/maturitessi-methode-2005-10-26.pdf

7. Tools supporting the method

Non commercial tools	Commercial tools
Yes, free of charge	

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Procurement

10. Flexible knowledge databases

Method allows use of sector adapted databases	Yes, domain specific vulnerabilities bases

17 ISF methods for Risk Assessment and Risk Management

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
ISF products concerning RA/RM refer often to each other and can be used complementarily. Such products are: • The Standard of Good Practice for Information Security • FIRM (Fundamental Information Risk Management) and the revised FIRM Scorecard • ISF's Information Security Status Survey • Information Risk Analysis Methodologies (IRAM) project • SARA (Simple to Apply Risk Analysis) • SPRINT (Simplified Process for Risk Identification)	Information Security Forum (ISF). ISF is an international association of over 260 leading companies and public sector organizations	International ISF members

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
		ISF member organizations	

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X		

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●● (IRAM, SARA, SPRINT)	
Risk analysis	●●● (IRAM, SARA, SPRINT)	
Risk evaluation	●●● (IRAM, SARA, FIRM Scorecard)	As a part of the IRAM project in the phase 1 "Business Impact Assessment" SARA, phase 4, step 4.1 "Analyze security exposures" The FIRM Scorecard collects information about criticality, vulnerabilities, level of threat connected to information resources and assesses the out coming business impact. Parts of the IRAM project such as the Business Impact Reference Table (BIRT) and relevant information from the Survey such as incident information are included in the Scorecard as well.

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●● (FIRM Scorecard, SARA, SPRINT)	
Risk treatment	●●● (The Standard of Good Practice)	The Standard of Good Practice provides a set of high-level principles and objectives for information security together with associated statements of good practice (controls).
Risk acceptance	●●● (The Standard of Good Practice)	
Risk communication	●●● (FIRM)	FIRM, Part 5 "Coherent roles and reporting lines"

Brief description of the product:

The Standard of Good Practice provides a set of high-level principles and objectives for information security together with associated statements of good practice. They can be used to improve the level of security in an organization in a number of ways.
The Standard of Good Practice is split into five distinct aspects, each of which covers a particular type of environment. These are:

- Security Management (enterprise-wide)
- Critical Business Applications
- Computer Installations ('Information Processing' in previous versions)
- Networks ('Communications Networks' in previous versions)
- Systems Development

FIRM is a detailed methodology for the monitoring and control of information risk at the enterprise level. It has been developed as a practical approach to monitoring the effectiveness of information security. As such it enables information risk to be managed systematically across enterprises of all sizes. It includes comprehensive implementation guidelines, which explain how to gain support for the approach and get it up and running. The Information Risk Scorecard is an integral part of *FIRM*. The *Scorecard* is a form used to collect a range of important details about a particular information resource such as the name of the owner, criticality, level of threat, business impact and vulnerability.

The *ISF's* Information Security Status Survey (the Survey) is a comprehensive Risk Management tool that evaluates a wide range of security controls used by organizations to control the business risks associated with their IT-based information systems.

SARA is a detailed methodology for analyzing information risk in critical information systems. It consists of 4 phases:

- Planning
- Identify Business Requirements for Security
- Assess Vulnerability and Control Requirements
- Report

SPRINT is a relatively quick and easy-to-use methodology for assessing business impact and for analyzing information risk in important but not critical information systems. The full *SPRINT* methodology is intended to be applied to important, but not critical, systems. It complements the Forum's *SARA* methodology, which is better suited to analyzing the risks associated with critical business systems.

SPRINT first helps decide the level of risk associated with a system. After the risks are fully understood, *SPRINT* helps determine how to proceed and, if the *SPRINT* process continues, culminates in the production of an agreed plan of action for keeping risks within acceptable limits. *SPRINT* can help:

- identify the vulnerabilities of existing systems and the safeguards needed to protect against them;
- define the security requirements for systems under development and the controls needed to satisfy them.

4. Lifecycle

Date of the first release	Date and identification of the last version
Different dates for different ISF products	The Standard of Good Practice for Information Security: newest version in 2005 The ISF's Information Security Status Survey: newest version in 2005 FIRM: newest version in 2005

5. Useful links

Official web site	Available only to ISF Members at http://www.securityforum.org
User group web site	
Relevant web site	

6. Languages

Availability in European languages	EN

7. Price

Free	Not free	Updating fee
	Membership required	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X		X	X
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Specialist	Specialist	Specialist

2. Consultancy support

Open market	Company specific
No	

3. Regulatory compliance
NA

4. Compliance to IT standards

ISO/IEC IS 17799

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

Is it possible to measure the I.S.S. maturity level?	No

7. Tools supporting the method

Non commercial tools	Commercial tools
ISF provides a variety of tools (Excel tables, lists and forms) for these products. These tools are available for ISF members only.	

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Under development

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

18 ISO/IEC IS 13335-2 (ISO/IEC IS 27005)

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
ISO/IEC IS 13335-2: Management of information and communications technology security - Part2: Information security Risk Management Remark: This standard is currently under development; completion is expected for 2006. Subject to endorsement of ISO JTC1 the title will change to ISO/IEC IS 27005 "Information security Risk Management"	ISO	International (organization based in Switzerland)

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
	ISO		

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X		X

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●	generic: chapter 5.2, examples: annex C, generic: chapter 5.2, 5.3, examples: annexes C, D
Risk analysis	●●	generic: chapter 5.2, examples: annex C
Risk evaluation	●●	generic: chapter 5.2, 5.3, examples: annexes C, D

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●●	generic: chapter 5, examples: annex D
Risk treatment	●●●	chapter 6, annex E
Risk acceptance	●●●	chapter 7
Risk communication	●●●	chapter 8

Brief description of the product:

ISO/IEC IS 13335-2 is an *ISO* standard describing the complete process of information security Risk Management in a generic manner. The annexes contain examples of information security Risk Assessment approaches as well as lists of possible threats, vulnerabilities and security controls. *ISO/IEC IS 13335-2* can be viewed at as the basic information Risk Management standard at international level, setting a framework for the definition of the Risk Management process.

4. Lifecycle

Date of the first release	Date and identification of the last version
1998 (former ISO/IEC TR 13335-3 and 13335-4)	A new version is currently under development and expected to be finished in 2006. Presumably the numbering and the title will change to ISO/IEC IS 27005 "Information security Risk Management", subject to endorsement of ISO JTC1 The current version as of January 2006: 1st CD

5. Useful links

Official web site	http://www.iso.org
User group web site	
Relevant web site	

6. Languages

Availability in European languages	EN

7. Price

Free	Not free	Updating fee
	Ca. € 100	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies

X	X	(X)	X	X
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To install	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Not necessary	

3. Regulatory compliance

NA

4. Compliance to IT standards

ISO/IEC IS 13335-1	ISO/IEC IS 17799	ISO/IEC IS 27001

5. Trial before purchase

CD or download available	Registration required	Trial period
Download available (when published), but not for free		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
No	No

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Yes

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

19 ISO/IEC IS 17799:2005

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
Information technology- Security techniques – code of practice for information security management	ISO	International (organization based in Switzerland)

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
	ISO		

3. Identification

R.A. Method	R.M. Method	National standard	International standard
			X

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●	Standard is a good practice for initial threat identification indirectly implied.
Risk analysis	-	Phase not explicitly handled in the document.
Risk evaluation	-	Phase not explicitly handled in the document.

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	-	Phase not explicitly handled in the document.
Risk treatment	●	Standard is a good practice for initial risk treatment indirectly implied.
Risk acceptance	-	Phase not explicitly handled in the document.
Risk communication	-	Phase not explicitly handled in the document.

Brief description of the product:

This standard is of UK origin, but adapted to the international needs via *ISO*. This document shows what should be good practices in information processing. It is neither a method for evaluation nor for management of risks although a generic chapter refers to this issue. The document enlists various points that have to be taken into account to manage an information

system suitably, even if some are not applicable within a specific company.

4. Lifecycle

Date of the first release	Date and identification of the last version
2000	2005, version 2

5. Useful links

Official web site	http://www.iso.ch
User group web site	
Relevant web site	http://www.17799.com/

6. Languages

Availability in European languages	UK, FR

7. Price

Free	Not free	Updating fee
	Ca. € 130 (CHF 200)	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	Yes

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Yes	

3. Regulatory compliance
NA

4. Compliance to IT standards

ISO/IEC IS 13335

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
	Many

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Human resource management, change management, business continuity planning, audit

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

20 ISO/IEC IS 27001 (BS7799-2:2002)

In October 2005 the ISO/IEC IS 27001 was published and replaced the British standard BS7799 part 2 as reference for certification processes (BS7799 will disappear as reference at the end of the certificates renewal process (ca. 2007-2008).

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
Information security management systems – Requirements	ISO (The former BS7799-2 was the responsibility of the British Standards Institute)	International (organization based in Switzerland)

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
	ISO		

3. Identification

R.A. Method	R.M. Method	National standard	International standard
			ISO/IEC IS 27001 published in October 2005 is the transposition of the BS7799-2 by ISO (including some modifications to meet international requirements)

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	-	Generic requirement that threat identification has to be made through a recognized method, but no support is provided.
Risk analysis	-	
Risk evaluation	-	

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments

Risk assessment	-	Generic requirement that Risk Assessment has to be made through a recognized method but no support is provided.
Risk treatment	●	Generic recommendation that risk treatment has to be made
Risk acceptance	●	Indirectly implied through "statement of applicability".
Risk communication	-	

Brief description of the product:

This standard is dedicated to a process of certification. It enables the comparison of an information security management system through a series of controls. This standard does not cover risk analysis or certification of the Risk Management. Of UK origin, this standard has been adopted by *ISO* with some modifications. A certificate granted according to this standard confirms the compliance of an organization with defined requirements to information security management and a set of security controls.

4. Lifecycle

Date of the first release	Date and identification of the last version
1993	2005

5. Useful links

Official web site	http://www.iso.org
User group web site	
Relevant web site	http://www.xisec.com http://www.17799.com

6. Languages

Availability in European languages	EN, FR

7. Price

Free	Not free	Updating fee
	Ca. € 80 (CHF 126)	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X			
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	Yes
Existing certification scheme	Yes

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Specialist	Standard	Standard

2. Consultancy support

Open market	Company specific
Yes	Yes

3. Regulatory compliance

NA

4. Compliance to IT standards

ISO/IEC IS 17799

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
	Many

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Human resource management, business continuity planning.

10. Flexible knowledge databases

Method allows use of sector adapted databases	In commercial tools

21 IT-Grundschutz (IT Baseline Protection Manual)

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
IT-Grundschutz (Former English name: IT Baseline Protection Manual)	Federal Office for Information Security (BSI)	Germany

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
BSI (Germany)			

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X	X	

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	Each IT-Grundschutz module contains a list of typical threats. Threats are also classified in 5 threat catalogues. Identification of additional threats takes place during the supplementary risk analysis. Risk characterization is the result of the assessment of protection requirements. For this purpose, protection requirement categories are defined and potential damage scenarios are assigned to these protection requirement categories. A further risk characterization is provided within the supplementary risk analysis, where risks are characterized with the help of the assigned decision of how to handle them (see Risk Analysis based on IT-Grundschutz, chapter 6, “Handling threats”).
Risk analysis	●●●	To each threat, contained in a module, a detailed description of the thread is provided.
Risk evaluation	●●●	An exposure assessment is made within the assessment of the protection requirements

		with the help of damage scenarios. For threats identified within the scope of a supplementary risk analysis, the exposure assessment takes place during the phase of threats assessment.

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●●	See RA method phases
Risk treatment	●●●	Catalogues of recommended safeguards. Detailed description of safeguards assigned to each IT-Grundschutz module. Assignment of safeguards to the threats considered (cross reference tables). Risk treatment alternatives, see Risk Analysis based on IT-Grundschutz, chapter 6, "Handling threats" in part C.
Risk acceptance	●●●	Risk analysis based on IT-Grundschutz, "Handling threats" in part C.
Risk communication	●●●	Risk communication is part of the module "IT security management" and especially handled within the safeguards S 2.191 "Drawing up of an Information Security Policy" and S 2.200 "Preparation of management reports on IT security"

Brief description of the product:

IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain. The IT security process suggested by IT-Grundschutz consists of the following steps:

- Initialization of the process:
  - Definition of IT security goals and business environment
  - Establishment of an organizational structure for IT security
  - Provision of necessary resources
- Creation of the IT Security Concept:
  - IT-Structure Analysis
  - Assessment of protection requirements
  - Modeling
  - IT Security Check
  - Supplementary Security Analysis

- Implementation planning and fulfillment
- Maintenance, monitoring and improvement of the process
- IT-Grundschutz Certification (optional)

The key approach in *IT-Grundschutz* is to provide a framework for IT security management, offering information for commonly used IT components (modules). *IT-Grundschutz* modules include lists of relevant threats and required countermeasures in a relatively technical level. These elements can be expanded, complemented or adapted to the needs of an organization.

4. Lifecycle

Date of the first release	Date and identification of the last version
1994	2005

5. Useful links

Official web site	http://www.bsi.de/gshb/index.htm http://www.bsi.de/english/gshb/index.htm
User group web site	
Relevant web site	

6. Languages

Availability in European languages	DE, EN

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Many

3. Level of detail

Management	X	Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	Yes
Existing certification scheme	Yes

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Yes	Yes

3. Regulatory compliance

KonTraG (German Act on Control and Transparency in Businesses)	Basel II	TKG (German Telecommunications Act)	BDSG (German Federal Data Protection Act)

4. Compliance to IT standards

ISO/IEC IS 17799	ISO/IEC IS 27001

5. Trial before purchase

CD or download available	Registration required	Trial period
Product is free		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	Yes (three levels)

7a. Tools supporting the method

Non commercial tools	Commercial tools
GSTOOL: free for public authorities	BSI - GSTOOL HiSolutions AG HiScout SME INFODAS GmbH - SAVe inovationtec - IGSDoku Kronsoft e.K. - Secu-Max Swiss Infosec AG - Baseline-Tool WCK - PC-Checkheft

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Quality management, IT revision, Data Protection, SLA management, Project management

10. Flexible knowledge databases

Method allows use of sector adapted databases	Yes

22 Marion

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
MARION: **M**éthodologie d'**A**nalyse des **R**isques **I**nformatiques et d'**O**ptimisation par **N**iveau	CLUSIF	France

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
		CLUSIF - Club de la Sécurité Informatique Français	

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X			

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	There is a predefined set of 17 types of threats
Risk analysis	●●●	Each threat is used against each asset
Risk evaluation	●●●	Step 2 of MARION is the vulnerability assessment, Step 3 of MARION is the risk analysis and the evaluation of the risk

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	-	
Risk treatment	-	
Risk acceptance	-	
Risk communication	-	

Brief description of the product:

The method *MARION* (Methodology of Analysis of Computer Risks Directed by Levels) arises from the *CLUSIF* (http://www.clusif.asso.fr/) and the last update was performed in

1998. It is based on a methodology of audit, which, as its name indicates, allows for estimating the level of IT security risks of a company through balanced questionnaires giving indicators in the form of notes on various subjects relative to security. The objective of the method is to obtain a vision of the company with regard to a level considered "correct", and on the other hand with regard to companies having already answered the same questionnaire. The level of security is estimated according to 27 indicators distributed in 6 large subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to ensure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is carried out to identify the risks (threats and vulnerabilities) that face the company.

Note: The *CLUSIF* does not sponsor this method anymore, as *MARION* is replaced by *MEHARI*. However, *MARION* is still used by various companies.

4. Lifecycle

Date of the first release	Date and identification of the last version
1990	1998 (not maintained anymore)

5. Useful links

Official web site	https://www.clusif.asso.fr/en/clusif/present/
User group web site	
Relevant web site	https://www.clusif.asso.fr/fr/production/catalog/index.asp

6. Languages

Availability in European languages	FR, EN

7. Price

Free	Not free	Updating fee
	One shot (price unknown)	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
	X			
Specific sector				

2. Geographical spread

Used in EU member states	FR, BE, LU
Used in non-EU countries	Switzerland, Canada (Quebec)

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Basic	Standard	Basic

2. Consultancy support

Open market	Company specific
Yes	

3. Regulatory compliance

NA

4. Compliance to IT standards

NA

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
No	MS Excel

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

23 Mehari

Mehari is the successor of Melisa. Mehari also replaces Marion, although the latter is still used.

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
MEHARI: Méthode Harmonisée d'Analyse de Risques Informatiques	CLUSIF	France

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
		CLUSIF - Club de la Sécurité Informatique Français	

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X			

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	12 types of scenarios exist (knowledge database), final evaluation of impact and potentiality
Risk analysis	●●●	Each scenario is tested (selection)
Risk evaluation	●●●	To complete the evaluation process of the risk

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	-	
Risk treatment	-	
Risk acceptance	-	
Risk communication	-	

Brief description of the product:

MEHARI is a risk analysis method, designed by security experts of the *CLUSIF*. It proposes an approach for defining risk reduction measures suited to the organization objectives.

MEHARI provides:

- a Risk Assessment model,
- modular components and processes.

MEHARI enhances the ability to:

- discover vulnerabilities through audit,
- analyze risk situations.

MEHARI includes formulas facilitating:

- threat identification and threat characterization,
- optimal selection of corrective actions.

4. Lifecycle

Date of the first release	Date and identification of the last version
1996	Nov 2004

5. Useful links

Official web site	https://www.clusif.asso.fr/en/clusif/present/
User group web site	
Relevant web site	https://www.clusif.asso.fr/fr/production/catalog/index.asp

6. Languages

Availability in European languages	FR, EN

7. Price

Free	Not free	Updating fee
	One shot (€100-€500)	

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	Many
Used in non-EU countries	Switzerland, Canada (Quebec)

3. Level of detail

Management	X	Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To install	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Yes	

3. Regulatory compliance

NA

4. Compliance to IT standards

ISO/IEC IS 17799	ISO/IEC IS 13335

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools
No	RISICARE (ca. € 10.000)

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	Corporate data bases

24 Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses)

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
OCTAVE v2.0, OCTAVE-S v1.0	Carnegie Mellon University, SEI (Software Engineering Institute)	USA

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
			Carnegie Mellon University (USA), CERT (Computer Emergency Response Team) http://www.CERT.org/octave/osig.html

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X		

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●	Criteria only
Risk analysis	●●	Criteria only
Risk evaluation	●●	Criteria only

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●	Criteria only
Risk treatment	●●	Criteria only
Risk acceptance	●●	Criteria only
Risk communication	●●	Framework

Brief description of the product:

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

4. Lifecycle

Date of the first release	Date and identification of the last version
Version 0.9, 1999	Version 2.0, January 2005

5. Useful links

Official web site	http://www.cert.org/octave/osig.html
User group web site	
Relevant web site	http://www.cert.org/octave General interest e-mail: octave-info@sei.cmu.edu Licensing: licensing-octave@sei.cmu.edu

6. Languages

Availability in European languages	EN

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
		X		
Specific sector				

2. Geographical spread

Used in EU member states	
Used in non-EU countries	USA

3. Level of detail

Management	X	Operational	X	Technical	

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific
Yes	

3. Regulatory compliance
NA

4. Compliance to IT standards
NA

5. Trial before purchase

CD or download available	Registration required	Trial period
Yes	Yes	No

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7a. Tools supporting the method

Non commercial tools	Commercial tools
	Licensed materials, Trainings

7b. Sector with free availability

Public related sectors	Others
	Educational Support, Awareness trainings

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	Information Assurance

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

25 SP800-30 (NIST)

A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin
Risk Management Guide for Information Technology systems	National Institute for Standards and Technology (NIST)	United States

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organization / association	Public / government organization
NIST (USA)			

3. Identification

R.A. Method	R.M. Method	National standard	International standard
X	X		

If R.A. method:

R.A. Method activities	Included? (-, ●..●●●)	Comments
Risk identification	●●●	Detailed with samples
Risk analysis	●●●	Detailed in check-list and with samples
Risk evaluation	-	

If R.M. method:

R.M. Method processes	Included? (-, ●..●●●)	Comments
Risk assessment	●●●	Very detailed with inventory and template
Risk treatment	●●●	Detailed with flowchart and with mathematical aspect
Risk acceptance	●●●	Include in a chapter on risk mitigation
Risk communication	-	

Brief description of the product:

This product is one of the *Special Publication 800-series reports*. It gives very detailed guidance and identification of what should be considered within a Risk Management and Risk Assessment in computer security. There are some detailed checklists, graphics (including flowchart) and mathematical formulas, as well as references that are mainly based on US regulatory issues.

4. Lifecycle

Date of the first release	Date and identification of the last version
2002	2002

5. Useful links

Official web site	http://www.csrc.nist.gov
User group web site	
Relevant web site	

6. Languages

Availability in European languages	EN

7. Price

Free	Not free	Updating fee
X		

B: Scope

1. Target organizations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
X	X	X	X	X
Specific sector				

2. Geographical spread

Used in EU member states	
Used in non-EU countries	USA

3. Level of detail

Management		Operational	X	Technical	X

4. License and certification scheme

Recognized licensing scheme	No
Existing certification scheme	No

C: Users viewpoint

1. Skills needed

To introduce	To use	To maintain
Standard	Standard	Standard

2. Consultancy support

Open market	Company specific

Yes	

3. Regulatory compliance
NA

4. Compliance to IT standards
NA

5. Trial before purchase

CD or download available	Registration required	Trial period
No		

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	No

7. Tools supporting the method

Non commercial tools	Commercial tools

8. Technical integration of available tools

Tools can be integrated with other tools	No

9. Organization processes integration

Method provides interfaces to other organizational processes	

10. Flexible knowledge databases

Method allows use of sector adapted databases	

ANNEX IV: Structure of template for tool description

In order to classify tools and in particular their level of visibility in the market and their main features and functions, a template similar to that used for method description has been introduced. Some modifications have been made to catch particular characteristics of tools, like tool architecture, supported functionality, interoperability etc.

Again, attributes in three categories have been grouped as follows:

D: "***Product Identity card***",
E: "***Product Scope***" and
F: "***Users viewpoint***".

Both attribute categories and attribute semantics are presented in the forthcoming sections.

25.1 A: Product identity card

1: General information

Basic information to identify the product. The information provided here contains the name of the product, the company or cross-frontier organization that provides the product and the country of origin in case the product originated from a company or national organization.

2: Level of reference of the product

Details about the type of initiator of the product:

- World-wide (state oriented)
- World-wide (sector oriented)
- Regional
- Local
- Sustained by organization, club

3: Brief description of the product

A brief description of the product containing general information, overview of function.

4: Supported functionality

Specifies the functionality this tool provides
R.A. Method activities supported: Does the tool provide Risk assessment functionality? If yes, specify the activities included and how they are supported.
R.M. Method processes supported: Does the tool provide Risk Management functionality? If yes, specify the processes included and how they are supported.

Other functionality: Does the tool provide any further functionality not included in the previous? If yes, specify and describe it.
Information Processed: Specify what kind of results/output this tool generates in each phase.

5: Lifecycle
Date of the first edition, as well as date and number of actual version.

6: Useful links
Official web site: hyperlink to the site of the originator/provider of the product, where to download the product or order it.
Related user group web site: hyperlink to the web site of the user group (if any) for the product.
Main relevant web site: web site that offers relevant and neutral information concerning the product.

7: Languages
Languages available: List the available languages that the tool supports

8: Pricing and licensing models
Free: the solution is free ("freeware").
Not free: specify the price for the different licensing models
Maintenance fee: the yearly fee for maintenance.
Sectors with free availability or discounted price: if the tool is not free, specify kind of organizations that it may be provided as free or have a price discount.

9: Trial
Details regarding the evaluation period of the tool (if it does exist).

10: Tool architecture
Specify the technologies used in this tool as well as how it is deployed (stand alone application, web application, database used…)

25.2 B: Scope

1: Target organizations
Defines the most appropriate type of organizations the product aims at:

- **Governments, agencies**: the product is developed for organizations working for a state (e.g. the NSA in USA).
- **Large companies**: the product is useful for companies with more than 250 employees.
- **SME**: the product is useful for small and medium size companies that cannot afford dedicated Risk Management personnel or complete segregation of duties.

- **Commercial companies**: the product is targeted to companies that have to implement it due to commercial demands from stakeholders, financial regulators, etc.
- **Non-profit**: companies where commercial benefits are not essential like the NGO's health sector, public services, etc.
- **Specific sector**: the product is dedicated to a very specific sector (e.g. nuclear) and usually cannot be used in other sectors.

2: Geographical spread

General information about the spread of the product including:
Used in European countries: list of EU member states in which implementation is known by working group members. This includes organization as:

- European institutions (e.g. European Commission, European Union Council, European agencies).
- International organizations situated in Europe (e.g. NATO, UNO, OECD, UNESCO).

Used in non-European countries: used within potential new member states of the European Union or outside the EU in other countries such as Switzerland or USA.

3: Level of detail

The targeted kind of users is:

- Management level: generic guidelines.
- Operational level: guidelines for implementation planning, with a low level of detail.
- Technical level: specific guidelines, concerning technical, organisational, physical and human aspects of IT Security with a high level of detail.

4: Compliance to IT Standards

List the national or international standard this tool is compliant with.

5: Certification

Specify whether the tool helps the company toward a certification according to a standard.

6 : Training

Information about possible training courses for this tool

25.3 C: Users viewpoint

1: Skills needed

The level of skills needed to implement and maintain the product (method or standard):

- **Basic level**: common sense and experience.
- **Standard level**: some days or weeks of training are sufficient.
- **Specialist level**: thorough knowledge and experience is required.

To install: the skills needed to install the necessary products.
To use: the specific qualifications needed in order to perform current work (documentation easy to understand, user-friendly interface, etc).
To maintain: is the product stable or are there regular updates that require specific education or regular training. (on a technical side: is it necessary to hire a specialist to perform the actions?)

2: Tool support

Specify the kind of support the company provides for this product.

3: Organization processes integration

Tool foresees different roles of users: Specify and explain if the tool supports roles of users
Tool delivers results that can be used by other processes/activities: Is it able for someone to use the results of this tool in another organization's activity?

4: Interoperability with other tools

Specify available interfaces or other ways of integration with other tools

5: Sector adapted knowledge database supported

Specify whether the tool provides a knowledge database specific for a sector

6: Flexibility

Specify whether it is possible to customize the tool's knowledge database to client requirements.

ANNEX V: Inventory of tools

26 Callio

26.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Callio Secura 17799	Callio technologies	Canada

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Callio Secura 17799 is a product from *Callio technologies*. It is a web based tool with database support that let the user implement and certify an information security management system (ISMS). It supports the ISO17799 and ISO 27001 (BS 7799-2) standards and can produce the documents that are needed for certification. Moreover it provides document Management functionality as well as customization of tool's databases. A trial version is available for evaluation.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Risk assessment module: identify vulnerabilities/threats, associate with assets Suggested list of threats
Risk analysis		
Risk evaluation	X	Risk evaluation & Risk calculation
Other phases		
Asset inventory & evaluation	X	Range of examples grouped in categories Evaluation of loss or damage

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	-
Risk treatment	X	Selection of ISO 17799 Controls: flexible list

		of suggested controls Create and evaluate different scenarios
Risk acceptance		
Risk communication	X	Document Management, Awareness Center Portal
Other phases		
ISO 17799 Preliminary Diagnostic	X	Questionnaire, initial judgment regarding the state of security
Policy management/Audit Preparation	X	Create security policy using proposed policies and directives
ISMS Diagnostic	X	Verify if the ISMS meets the requirements for BS 7799-2 certification

Other functionality:

Name	Description
Document Management	ISMS documentation requirements Document approval system & version control Document templates
Reports Tool	Automatic report generator
Glossary	Glossary of information security terms
Awareness Center portal	Publish information security documents for different staff member groups.

Information processed

Name	Description
ISMS	ISMS goal and scope
ISO 17799	USI 17799 compliance report
Inventory of Assets	Inventory and evaluation of the assets to be protected
Risk Analysis	Identification and evaluation of threats vulnerabilities and requirements, Risk calculation
Risk Treatment	Risk treatment plan outline
Statement of applicability	Controls and ISMS
Customized security policies	Personalized policies and templates

5. Lifecycle

Date of first release	Date and identification of the last version
2001	2005 – version 2

6. Useful links

Official web site	www.callio.com
User group web site	-

(optional)	
Relevant web site:	-

7. Languages

Languages available	Fr	UK	Es						

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	4,495 € (2 users license) 6,495 € (5 users license) 9,995 € (10 users license) 1495 $ per additional user	Euros / percentage	-
Sectors with free availability or discounted price				
-				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Web demo & download	Yes	-

10. Tool architecture

Technical component	Purpose	Comment
Database	Store information	MySQL, SQL Server
Web server	Serve the content	IIS, Apache
Application Server	Run the application	BlueDragon JX Server
Client	-	Internet Explorer

26.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X	X	X	
Specific sector :	-			

2. Spread

General information	World-wide in many different organizations								
Used inside EU countries	-								
Used outside EU countries	Canada	Mexico	Taiwan						

3. Level of detail

Level	Tool functions	Comment
Management		

Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 17799	Verify level of compliance	Gap analysis
ISO 27001 (BS 7799-2)	Verify if ISMS meets requirements for certification	-

5. Tool helps towards a certification

Certification according to standard	Comments
ISO 27001 (BS 7799-2)	-

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

26.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Easy to install : Web application installed on company server
To use	Simple interface, easy to be used, online help system
To maintain	No updates required

2. Tool support

Support method	Comment
Support (telephone, email)	1 year, 20% of license price

3. Organization processes integration

Role	Functions
NA	NA

4. Interoperability with other tools

Integration Method	Tools
SQL Database	Report Generators (Crystal Reports…)

5. Sector adapted knowledge databases supported

Database Name	Contents
NA	NA

6. Flexibility of tool's database

Database Name	Comments

List of controls, vulnerabilities, threats	Customize the list
Questionnaire	Import client specific questionnaire Customize questionnaires

27 Casis

27.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Casis	Aprico Consultants	Belgium

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

CASIS software is an "Advanced Security Audit Trail Analyzer", meaning that its purpose is the collection of log file data across multiple systems, correlation of these data and production of security alerts based on user defined rules. The user is able to define new sources of data as well as to specify the alert output. *CASIS* is a product of *Aprico Consultants*.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification		
Risk analysis		
Risk evaluation		
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment		
Risk treatment		
Risk acceptance		
Risk communication		
Other phases		

Other functionality:

Name	Description

Collect data	Collect native audit data from systems or applications
Clean and transform	Filter data, transform to structured data, store in database
Generate alerts	Generate alerts by using rule-based correlation of events, statistical models and data mining algorithms
Alert notification	

Information processed

Name	Description

5. Lifecycle

Date of first release	Date and identification of the last version
-	-

6. Useful links

Official web site	www.aprico-consult.com/corporate/index.htm www.casissecurity.com
User group web site (optional)	
Relevant web site:	

7. Languages

Languages available	EN								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	Based on different parameters (volume of treated logs, number of application domains, number of installations, number of sites). The current list price starts from 45.000 €	Euros / percentage	€
Sectors with free availability or discounted price				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Under consideration	-	-

10. Tool architecture

Technical component	Purpose	Comment

Database	Store collected data	Oracle, SQL Server, MySQL
Application	Main functionality	JAVA, XML (JAXP)

27.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
	X	X		
Specific sector :				

2. Spread

General information								
Used inside EU countries	Belgium	France						
Used outside EU countries								

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
-	-	-

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

27.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	NA
To use	NA
To maintain	NA

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Risk ETL	Collects raw audit trail information from any source (applications, operating systems, security devices and access control equipment producing audit logs, etc)
SQL interface	SQL queries for interaction with other applications

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
Collecting formats	Creation of new collecting formats
Correlation rules	High level language used to specify rules for the Rules Correlation Engine

28 Cobra

28.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Cobra	C&A Systems Security	UK

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Cobra software tool enables security Risk Assessment to be undertaken by organizations themselves. It evaluates the relative importance of all threats and vulnerabilities, and generates appropriate solutions and recommendations. It will automatically link the risks identified with the potential implications for the business unit. Alternatively, a particular area or issue can be examined 'stand alone', without any impact association. COBRA comes equipped with four discrete knowledge bases that can be further customized using the Module Manager component.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Identify system threats, vulnerabilities and exposures. Measure the degree of actual risk for each area or aspect of a system, and directly link this to the potential business impact.
Risk analysis		
Risk evaluation	X	Identify system threats, vulnerabilities and exposures
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	

Risk treatment	X	Offer detailed solutions and recommendations to reduce the risks.
Risk acceptance		
Risk communication	X	Provide business as well as technical reports.
Other phases		

Other functionality:

Name	Description
ISO 17799 compliance check	COBRA ISO17799 Consultant component

Information processed

Name	Description
Reports	-

5. Lifecycle

Date of first release	Date and identification of the last version
90s	Release 3

6. Useful links

Official web site	http://www.riskworld.net/
User group web site (optional)	
Relevant web site:	

7. Languages

Languages available	EN								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	x	Full Cobra Suite: $1995 Cobra for ISO17799: $895	Euros / percentage	
Sectors with free availability or discounted price				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Evaluation copy available	Yes	-

10. Tool architecture

Technical component	Purpose	Comment
Application	-	Stand alone tool

28.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
		X	X	
Specific sector :				

2. Spread

General information	N/A									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 17799	-	COBRA ISO17799 Consultant : Checking compliance with the ISO 17799 security standard

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

28.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Stand alone application, single installation
To use	Easy to use, On-line help, can be used without the need for detailed security knowledge or expertise in using Risk Management software
To maintain	No updates needed

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
-	-

5. Sector adapted knowledge databases supported

Database Name	Contents
e-Security knowledge base	Specifically constructed to cover modern network based systems

6. Flexibility of tool's database

Database Name	Comments
Core knowledge database	Module manager: change questions, countermeasures, profiles, reports, etc

29 CounterMeasures

29.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
CounterMeasures	Alion	USA

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
X			
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Allion's product *CounterMeasures* performs Risk Management based on the US-NIST 800 series and OMB Circular A-130 USA standards. The user standardizes the evaluation criteria and using a "tailor-made" assessment checklist, the software provides objective evaluation criteria for determining security posture and/or compliance. *CounterMeasures* is available in both networked and desktop configurations and can be evaluated through a flash demonstration and a trial version.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Survey module/Data collection
Risk analysis	X	Analysis platform
Risk evaluation	X	Analysis platform
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Cost Benefit Analysis /Remediation Tracking
Risk acceptance	X	Cost Benefit Analysis /Remediation Tracking
Risk communication	X	CM Report suite
Other phases		

Other functionality:

Name	Description

Information processed

Name	Description
Survey data	Data collected at the data collection phase
Risks report	Description of risks associated with operations
Remediation plan	Plan of actions for facility security improvement
Residual risk	Figures

5. Lifecycle

Date of first release	Date and identification of the last version
mid 1980's	January 2006 – v8

6. Useful links

Official web site	www.countermeasures.com
User group web site (optional)	
Relevant web site:	www.alionscience.com

7. Languages

Languages available	En								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	Enterprise Platform : $14500 Standard Platform : $3990 Web Survey : $2500	Euros / percentage	
Sectors with free availability or discounted price				
Educational, Government				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Evaluation copy Flash demonstration	-	-

10. Tool architecture

Technical component	Purpose	Comment
Standalone application		
Web server		

29.2 B: Scope

1: Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X			
Specific sector :	Banks, Gas/Oil, Insurance, Ports, Universities, States/Municipalities, Security Firms			

2. Spread

General information										
Used inside EU countries										
Used outside EU countries	USA									

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
US-NIST 800 series		
OMB Circular A-130		

5. Tool helps towards a certification

Certification according to standard	Comments

6. Training

Course	Duration	Skills	Expenses
Training	2 days	Training on software and its application	Included in price

29.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Fully automated installation
To use	Simple interface, easy to use, Online help
To maintain	

2. Tool support

Support method	Comment
Support (Helpdesk)	One year, included in price, (includes also upgrades/enhancements) (after first year, 15% of the software purchase price)

3. Organization processes integration

Role	Functions

Result	Activity

4. Interoperability with other tools

Integration Method	Tools
Export	MS Excel
Results output	Results can be saved in database format

5. Sector adapted knowledge databases supported

Database Name	Contents
Physical Security	
Critical Infrastructure	
Seaport Security Risks	
Anti-Terrorism Force Protection	

6. Flexibility of tool's database

Database Name	Comments
Security databases	Create new / Customize
Threats / Assets / Vulnerabilities / Controls	Configure/ Customize

30 Cramm

30.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Cramm	Insight Consulting	UK

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

The *Cramm tool* provides an easy way to implement the *Cramm method*, developed by *Insight Consulting*. All three stages of the method are fully supported using a staged and disciplined approach. The tool comes in three versions: CRAMM expert, CRAMM express and BS 7799 Review. A trial version is available for evaluation.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Stage II
Risk analysis	X	Stage II
Risk evaluation	X	Stage II
Other phases		
Asset Identification	X	Stage I : Identify assets & evaluation

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Stage III
Risk acceptance		
Risk communication		
Other phases		

Other functionality:

Name	Description

BS 7799 Review	Assists in demonstrating compliance against BS 7799 / ISO 27001

Information processed

Name	Description

5. Lifecycle

Date of first release	Date and identification of the last version
1985	2005 - v5.1

6. Useful links

Official web site	www.cramm.com
User group web site (optional)	
Relevant web site:	www.crammgebruikersgroep.nl

7. Languages

Languages available	UK	NL	CZ						

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	CRAMM expert : £2950 per copy plus £875 annual license CRAMM express: £1500 per copy plus £250 annual license	Euros / percentage	
Sectors with free availability or discounted price				
UK Government, NATO, UK local authority, NHS, Academic				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Evaluation copy	Yes	30 days

10. Tool architecture

Technical component	Purpose	Comment
Standalone tool		

30.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs

X	X	X		
Specific sector :				

2. Spread

General information	Over 5000 different users in 23 countries									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards
List the national or international standard this tool is compliant with.

Standard	Compliance notice	Comment
BS 7799 (ISO 27001)		

5. Tool helps towards a certification

Certification according to standard	Comments
BS 7799	-

6. Training

Course	Duration	Skills	Expenses
CRAMM Training	3 days	risk analysis and management process, CRAMM method and software	£1195

30.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Simplified installation procedures
To use	CRAMM expert needs knowledge of the CRAMM method, CRAMM express can be used by someone who has never used CRAMM before
To maintain	-

2. Tool support

Support method	Comment
Helpdesk	Telephone, email

3. Organization processes integration

Role	Functions
-	-

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Reports export	MS Word / MS Excel/ MS Graph

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
-	-

31 Ebios

31.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Ebios	Central Information Systems Security Division (France)	France

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)	Club Ebios		

3. Brief description of the product

Ebios is a software tool developed by *Central Information Systems Security Division (France)* in order to support the *Ebios method.* The tool helps the user to produce all risk analysis and management steps according the five EBIOS phases method and allows all the study results to be recorded and the required summary documents to be produced. The *Ebios tool* is open source and free.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Step 3 of EBIOS method: 3.1 Study of threat sources Step 4 of EBIOS method: Identification of security objectives
Risk analysis	X	Step 3 of EBIOS method: 3.2 Study of vulnerabilities
Risk evaluation	X	Step 3 of EBIOS method: 3.3 Formalization of threats
Other phases		
Context Study	X	Step 1 of EBIOS method : Identify target system, general information, context of use, determine entities
Expression of security needs	X	Step 2 of EBIOS method: risk estimation and definition of risk criteria

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Step 4 of EBIOS method: Identification of security objectives Step 5 of EBIOS method: Determination of security requirements
Risk acceptance		Step 4 of EBIOS method: 4.2 List of residual risks
Risk communication	X	Reports produced for every step of the method
Other phases		

Other functionality:

Name	Description
Glossary	List of terms
References	List of reference documents

Information processed

Name	Description
Presentation of the organization	-
List of elements/entities	-
List of security rules	-
Security needs	-
List of threats	-
List of retained threats	-
List of residual risks	-

5. Lifecycle

Date of first release	Date and identification of the last version
1995	2004 – v2

6. Useful links

Link for further information

Official web site	www.ssi.gouv.fr/en/confidence/ebiospresentation.html
User group web site (optional)	-
Relevant web site:	-

7. Languages

Languages available	FR	ES	UK	DE					

8. Pricing and licensing models

Free	Not free	Maintenance fees

X	-	-	Euros / percentage	-
Sectors with free availability or discounted price				
-				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Full application free download	No	-

10. Tool architecture

Technical component	Purpose	Comment
Application	-	Stand alone application (Java & XML), Single installation

31.2 B: Scope

1. Target organizations

Defines the most appropriate type of communities for this tool

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X	X	X	X
Specific sector :	-			

2. Spread

General information	More than one thousand known uses (public and private sector)							
Used inside EU countries	France	Belgium	Luxembourg					
Used outside EU countries	Quebec	Tunisia						

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 13335	-	-
ISO 15408	-	Best practices included in knowledge database
ISO 17799	-	Best practices included in knowledge database

ISO 27001	-	-

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
Training in EBIOS method (by CFSSI)	2 days	Implementation practices Discuss issues on method Case studies	-

31.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	No installation needed, stand alone application
To use	Usable interface, help functionality, tutorial case provided Knowledge of the EBIOS method needed
To maintain	No updates needed

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Import/Export	HTML format (Custom made tools)

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
Questionnaires	Customize
List of Threats/Attacks/Vulnerabilities	Customize

32 GSTOOL

32.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
GSTOOL	Federal Office for Information Security (BSI) Germany	Germany

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

GStool has been developed by *Federal Office for Information Security (BSI)* in order to support users of the IT Baseline Protection Manual. After collecting the information required, the users have a comprehensive reporting system at their disposal for carrying out structure analyses on all of their compiled data and for generating reports on paper or in electronic form. *GSTOOL* is a stand-alone application with database support. A trial version is available.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Assessment of Protection Requirements
Risk analysis	X	Assessment of Protection Requirements
Risk evaluation	X	Assessment of Protection Requirements
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Baseline Protection Modeling, Basic Security Check, Supplementary Security Analysis
Risk acceptance	X	Estimation of cost and effort, residual risk
Risk communication	X	Reports Module
Other phases		

Other functionality:

Name	Description
IT Baseline Protection Certificate	Show qualification level that has been achieved

Information processed

Name	Description

5. Lifecycle

Date of first release	Date and identification of the last version
1998	2004 -v 3.1

6. Useful links

Official web site	www.bsi.bund.de/english/gstool www.bsi.bund.de/gstool
User group web site (optional)	
Relevant web site:	

7. Languages

Languages available	DE	EN							

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	1 license: 887,4 € 2 licenses: 1.774,80 € 3 licenses: 2.528,80 € 4-5 licenses: 3.990,40 € 6-10 licenses: 7.424,00 € 11-20 licenses: 13.572,00 € 21-40 licenses: 23.200,00 € More than 40 licenses: on request	Euros / percentage	
Sectors with free availability or discounted price				
German universities receive a 50% discount				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Evaluation version	No	30

10. Tool architecture

Technical component	Purpose	Comment

Standalone application		
Database		Microsoft MSDE, Microsoft SQL-Server

32.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X	X	X	X
Specific sector :				

2. Spread

General information	N/A									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
IT Baseline Protection Manual		

5. Tool helps towards a certification

Certification according to standard	Comments
IT Baseline Protection Certificate	

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

32.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Install wizard, single installation
To use	Detailed user manual

To maintain	

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity

4. Interoperability with other tools

Integration Method	Tools
-	-

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
Modules/'Threats/Safeguards	Edit, delete, add new

33 ISAMM

33.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
ISAMM	Telindus (Evosec)	Belgium

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
	X		
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Isamm is a Risk Management tool from *Telindus*. It calculates an ideal security remediation plan containing all relevant actions sorted on the basis of their ROSI (Return on Security Investment). ISAMM Risk Assessments are today proposed as consultancy services and guided assessments. A tool has been developed for internal use by *Telindus* consultants.

Enterprises of all kinds and all sizes can take advantage of the ISAMM methodology. The methodology is optimized so it can be used to assess very quickly the status of the security in a SME. On the other end large organizations can use ISAMM to systematically and periodically assess the risks of many information assets.

ISAMM Risk Assessments are today proposed as consultancy services and guided assessments. A tool has been developed for internal use by the Telindus consultants.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Relevant threats and applicable security policies & good practices are selected
Risk analysis	X	Threats are evaluated and the compliance with good practices is measured (periodically process)
Risk evaluation		
Other phases		
Asset Inventory	X	Most critical information resources in the company are identified

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Improvement plan is implemented and monitored
Risk acceptance	X	
Risk communication		
Other phases		

Other functionality:

Name	Description

Information processed

Name	Description
Security controls	A list of recommended security controls sorted on the basis of their ROSI (Return on Security Investment)
Security indicators	Projected security indicators that simulate the effect of the implementation of the security recommendations
Evolution of risks	Various graphs that represent the evolution of risks with the realization of security controls

5. Lifecycle

Date of first release	Date and identification of the last version
2002	2002(?)

6. Useful links

Official web site	http://www.evosec.be/isamm.htm (old)
User group web site (optional)	-
Relevant web site:	http://www.telindus.com/

7. Languages

Languages available									

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	N/A	Euros / percentage	
Sectors with free availability or discounted price				
-				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Possibilities for testing versions or pilot projects can be discussed with company.	-	-

10. Tool architecture

Technical component	Purpose	Comment
N/A	-	-

33.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X	X		
Specific sector :				

2. Spread

General information	N/A									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 17799	-	Best practices can be used

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

33.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	
To use	
To maintain	

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Export to spreadsheet	ISAMM results can be transferred into an Excel spreadsheet and can be linked with other Microsoft Office tools
Assessment management system	(on process)

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
Threads list	Customize
Security Controls list	Customize (ISO17799:2005 and ISF controls are built per default within ISAMM)

34 Octave Automated Tool

34.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Octave Automated Tool	Advanced Technology Institute (ATI)	USA

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
		X	
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Octave Automated Tool has been implemented by *Advanced Technology Institute (ATI)* to help users with the implementation of the Octave and Octave-S approach. The tool assists the user during the data collection phase, organizes collected information and finally produces the study reports. A demonstration as well as a trial version is available for evaluation.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Phase 1: Process 1-4, Phase2: Process 2
Risk analysis	X	Phase2: Process 1
Risk evaluation	X	Phase2: Process 1
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Phase3
Risk acceptance	X	Phase2: process 2
Risk communication		
Other phases		

Other functionality:

Name	Description

Information processed

Name	Description
List of critical assets / threats	
List of risks	
List of protection strategies	

5. Lifecycle

Date of first release	Date and identification of the last version

6. Useful links

Official web site	http://oattool.aticorp.org/Tool_Info.html
User group web site (optional)	
Relevant web site:	http://www.aticorp.org/

7. Languages

Languages available	EN								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	$1500 per instance	Euros / percentage	
Sectors with free availability or discounted price				
State or federal government				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Trial version & demonstration	Yes	-

10. Tool architecture

Technical component	Purpose	Comment
Standalone application		
Database		Microsoft Access

34.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs

X	X	X	X	X
Specific sector :				

2: Spread

General information	N/A									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
OCTAVE / OCTAVE-s		some of the features from OCTAVE-S

5. Tool helps towards a certification

Certification according to standard	Comments

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

34.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	
To use	Online help, knowledge of the OCTAVE method needed
To maintain	

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity

4. Interoperability with other tools

Integration Method	Tools
Reports Export	MS Word & Excel
Reports Export	Oracle database (built for US government)

5. Sector adapted knowledge databases supported

Database Name	Contents

6. Flexibility of tool's database

Database Name	Comments
Survey	Replaced some of the interview sessions with an organization focused survey

35 Proteus

35.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Proteus	Infogov (Information Governance Limited)	UK

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
		X	
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

Proteus Enterprise is a product suite from *Infogov*. Through its components the user can perform gap analysis against standards such as ISO 17799 or create and manage an ISMS according to ISO 27001 (BS 7799-2). The tool is web-based with database support and may be evaluated though a trial version.

Proteus Compliance provides a comprehensive and structured framework with which organizations can perform a gap analysis to identify and act upon weaknesses in the information security management systems.

Proteus Manager allows the creation and management of an ISMS according to BS 7799-2 (ISO 27001).

The web-server design makes deployment, access, workflow management and audit simple and efficient as possible whilst retaining central coordination.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	
Risk analysis	X	
Risk evaluation		
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Risk Treatment Plan
Risk acceptance		
Risk communication	X	Proteus WBT (Web Based Training) Module
Other phases		

Other functionality:

Name	Description
Remote auditing	Distribute questionnaires
Automated compliance analysis	Automatic produce key documents and reports

Information processed

Name	Description

5. Lifecycle

Date of first release	Date and identification of the last version
1999	2004

6. Useful links

Official web site	http://www.infogov.co.uk/proteus
User group web site (optional)	-
Relevant web site:	-

7. Languages

Languages available	EN								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	Compliance Lite:599 £/year Compliance Consultant:6000£/year or 600£/month Compliance SME: 2500£/year Compliance Corporate: available on request Manager: available on request	Euros / percentage	Included in price
Sectors with free availability or discounted price				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Evaluation version available	Yes	

10. Tool architecture

Technical component	Purpose	Comment
Server	-	ISS or Apache/ PHP
Database	-	MySQL
Client	-	Internet Explorer / Mozilla

35.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
	X	X	X	
Specific sector :				

2. Spread

General information	600 clients in 40 countries									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
BS 7799-2 (ISO 27001)		Proteus Manager
ISO 17799	Gap Analysis	Proteus Compliance

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses

-	-	-	-

35.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Rapid deployment via Intranet or secure Internet
To use	Easy to use without need for training
To maintain	Maintenance included (done by infogov)

2. Tool support

Support method	Comment
Maintenance	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
-	-

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
-	-

36 Ra2

36.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
RA2 art of risk	AEXIS	Germany

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

RA2 art of risk is a stand-alone tool from *AEXIS* for Risk Management based on the ISO 17799 and ISO 27001 standards. For each of the steps in this process the tool contains a dedicated step with report generation and printing out of the results. *RA2 Information Collection Device,* a component that is distributed along with the tool, can be installed anywhere in the organization as needed to collect and feed back information into the Risk Assessment process. *AEXIS* provides a trial version of the tool.

RA2 art of risk addresses the different steps in the process of establishing and implementing an ISMS, in accordance with the requirements lined out in the international standard *ISO/IEC 27001:2005* (previously *BS 7799-2:2002*). For each of the steps in this process the tool contains a dedicated step with a report generation and printing out of the results. With the tool, it is possible to go through all the steps described in ISO/IEC 27001:2005 and to produce the necessary documentation of the Risk Assessment and Risk Management process.

The functions include leading through the ISMS processes, calculation of risks, automatic carrying forward and updating of results, a detailed Help function and context sensitive help, and further support. Together with the tool *RA2* art of risk V1.1 comes the *RA2* Information Collection Device, which can be installed anywhere in the organization as necessary to collect and feed back information into the Risk Assessment process.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Example list of threats/vulnerabilities
Risk analysis	X	Risk decision process
Risk evaluation		
Other phases		

Asset inventory	X	Develop an ISMS asset inventory, select from example list, add new

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Suggested controls from ISO 17799, customization
Risk acceptance		
Risk communication	X	Report generator, print-out facility
Other phases		
ISMS Definition	X	Definition of the scope and business requirements policy and objectives for the ISMS

Other functionality:

Name	Description
Information Collection Device	Collect information from different sources within the organization. and feed back in the Risk Assessment process.

Information processed

Name	Description
Reports	Each step contains a report generation

5. Lifecycle

Date of first release	Date and identification of the last version
2000	2005 -v1.1

6. Useful links

Official web site	www.aexis.de/RA2ToolPage.htm
User group web site (optional)	-
Relevant web site:	www.bsi-global.com/Risk/InformationSecurity/bip0022.xalter

7. Languages

Languages available	EN(?)							

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	£ 1100 (plus VAT) v1.1 £ 200 (plus VAT) upgrade to v1.1	Euros / percentage	-
Sectors with free availability or discounted price				

-

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Demo Download	No	-

10. Tool architecture

Technical component	Purpose	Comment
Application	-	Stand alone application Installed in single machine
Information Collection Device	Collect information from different sources and provide as input to the tool	Multiple Installations in the organization / company

36.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
	X	X	X	X
Specific sector :				

2. Spread

General information	Applied around the world						
Used inside EU countries	France	Germany	Sweden	UK			
Used outside EU countries	Australia	Brazil	Canada	Japan			

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 27001 (BS 7799-2)	-	-
ISO 17799	-	-

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
-	-	-	-

36.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	Easy to install
To use	(?) help assistant, built in checklists, fully worked thought example
To maintain	Stable, no need for regular updates

2. Tool support

Support method	Comment
-	-

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Import/Export (application specific)	Information Collection Device
Export to CSV	Spreadsheet applications (e.g. Excel)

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
Assets/Threats/Vulnerabilities list	Customization of the list, define new
Controls list	Select 2000 or 2005 version list, identify additional controls

37 RiskWatch

37.1 A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
RiskWatch for Information Systems & ISO 17799	RiskWatch	USA

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
			X
Supported by organization, club,…(e.g. as sponsor)			

3. Brief description of the product

RiskWatch for Information Systems & ISO 17799 is the of RiskWatch company' solution for IS Risk Management. This tool conducts automated risk analysis and vulnerability assessments of information systems. The knowledge databases that are provided along with the product are completely customizable by the user, including the ability to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. The tool includes controls from the ISO 17799 and US-NIST 800-26 standards. RiskWatch provides an online demonstration of this product.

4. Supported functionality

R.A. Method activities supported:

R.A. Method activities	Included or not?	Comments
Risk identification	X	Phase I & II: List of predefined threats grouped in categories
Risk analysis	X	Phase I & II: Determine the potential financial impact
Risk evaluation	X	Phase I & II: Gather information about vulnerabilities
Other phases		

R.M. Method processes supported:

R.M. Method processes	Included or not?	Comments
Risk assessment	X	
Risk treatment	X	Phase III : Define safeguard details

Risk acceptance	X	Phase III : "what-if" scenarios
Risk communication		
Other phases		

Other functionality:

Name	Description
Asset Inventory	List of individual assets grouped in categories

Information processed

Name	Description
Executive Summary	-
Full and summary reports	For elements identified in Phases 1 and 2
Cost Benefit Report	-
Safeguard threat report	-
Audit trail reports	-
Final management report	-

5. Lifecycle

Date of first release	Date and identification of the last version
	2002 - version 9

6. Useful links

Official web site	http://www.riskwatch.com/isa.asp
User group web site (optional)	
Relevant web site:	

7. Languages

Languages available	En								

8. Pricing and licensing models

Free	Not free		Maintenance fees	
	X	$15.000	Euros / percentage	
Sectors with free availability or discounted price				
Educational discount: 25%				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)
Online demonstration	Yes	-

10. Tool architecture

Technical component	Purpose	Comment

Web server		
Standalone application		

37.2 B: Scope

1. Target organizations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
X	X	X		
Specific sector :				

2. Spread

General information	3000 users									
Used inside EU countries										
Used outside EU countries										

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment
ISO 17799	-	Control standards included
US-NIST 800-26	-	Control standards included

5. Tool helps towards a certification

Certification according to standard	Comments
-	-

6. Training

Course	Duration	Skills	Expenses
RiskWatch for Information Systems Two-Day Training	2 days	Principles of Risk Assessment, Familiarity with the RiskWatch Automated Risk Assessment Program,	$1000 per person
On-site Riskwatch training	2 days	Risk analysis with Riskwatch	$5500 per class

37.3 C: Users viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	
To use	On-line help,
To maintain	

2. Tool support

Support method	Comment
Online and telephone Support	Help, FAQ, etc

3. Organization processes integration

Role	Functions
-	-

Specify whether it is possible to use the tool's output in another organization's activity

Result	Activity
-	-

4. Interoperability with other tools

Integration Method	Tools
Import/Export	DataSheet (Excel), Databases (ODBC)

5. Sector adapted knowledge databases supported

Database Name	Contents
-	-

6. Flexibility of tool's database

Database Name	Comments
RiskWatch IS database	Create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets.

ANNEX VI: Structure used for the work on Risk Management at ENISA

In this annex, a logical structure of Risk Management as seen by ENISA, for analysis, planning and implementation purposes is developed. This structure will help readers understand the context of the present document and to follow updates/ expansions/ amendments to be released in the future, e.g. the open issues presented in this document.

37.4 Structure used for Risk Management

For the sake of classification of the various issues related to Risk Management, a hierarchical structure that depicts various views and dimensions of this topic has been established. This structure is graphically presented by the pyramid of Figure 5.

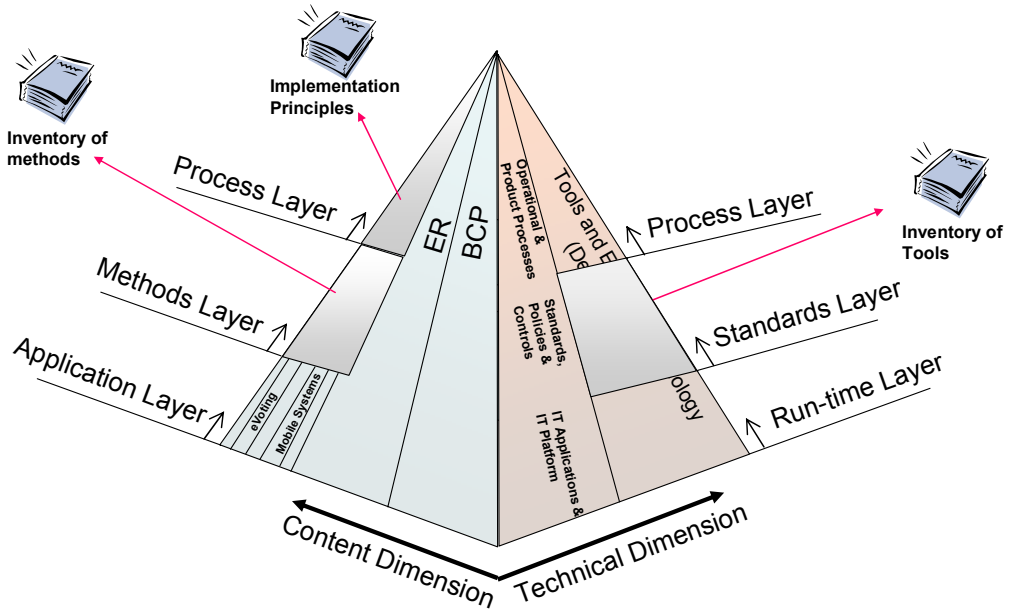

Figure 5: Hierarchical decomposition of Risk Management

As shown in this figure, the **content dimension of Risk Management** is divided into three sectors, each one related to a particular category of risk, namely:

- *Information Security Risks* are covered in the pyramid sector called Information Security Risk Management/Risk Assessment (**IS RM/AR**)
- *Emerging Risks* are covered in the sector called **ER** and

- *Availability Risks* are covered in the sector called Business Continuity Planning (**BCP**).

The **technical dimension of Risk Management** is orthogonal to the content dimension and represents all necessary efforts to map/integrate/implement the content of Risk Management by using technical components. It is divided into two sectors depicting two main activities namely:

- Integration of *Risk Management with* components from *Business Processes, Standards and IT-Applications* (depicted through the left sector in the technical dimension) and

- Installation of automated *Tools and generation of demonstrators.*

Further to the vertical fragmentation of Risk Management, the issues involved are refined through a decomposition scheme. This is represented via the horizontal layers of the pyramid. Accordingly, an issue on a higher level of the pyramid is logically decomposed by its subordinate level. The **content dimension of Risk Management** is divided into the three following layers:

- The **Process Layer** contains generic descriptions of the particular Risk Management issue consisting, for example, of process descriptions, activity descriptions, general terminology and so on. **By presenting a general overview, the present document corresponds to the documentation of the Process Layer for the Information Security Risk Management / Risk Assessment (IS RM/RA)** (s. Figure 5),

- The **Methods Layer** contains descriptions of existing methods in the relevant field based on dedicated templates. This information can be used for various purposes, e.g. as information material, as basis for comparisons of existing methods etc. **The inventory of methods attached to this document corresponds to this layer** (s. Figure 5) and

- The **Application Layer** contains information relevant to the deployment of a method from the previous layer for a certain IT-application. In the figure, this is illustrated by means of examples of IT-applications (e.g. eVoting, Mobile Systems), assessed though the Risk Management methods EBIOS [EBIOS] or ISO 13335 [ISO 13335-2]. ENISA plans to conduct such assessments in the future.

Similarly, the **technical dimension of Risk Management** is divided into three layers. These layers are:

- A **Process Layer** that stands for the integration of Risk Management into the processes of an organization (e.g. operational or product processes). As for tools,

this layer contains methods to integrate tool functionality into other operational processes.

- A **Standards Layer** that represents the policies, measurements and organizational controls mentioned in various security standards and implements those measurements in various technical platforms. As for tools, this layer contains information about the functionality and structure of tools. **The inventory of Risk Management / Risk Assessment Tools attached to this document is the instantiation of this layer for the content sector Information Security Risk Management / Risk assessment (IS RM/RA)** (s. Figure 5),

- A **Run-time Layer** that stands for all kinds of enabling technologies needed to run an IT-application (including the various run-time application modules). Concerning tools, this layer includes run-time environments of installed tools to facilitate Risk Management and Risk Assessment methods.