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

30/03/2006

Content

Preamble

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

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

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

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

3. Propose a roadmap document.

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

1. Executive summary

1.1 Summary

The working group (WG) on risk assessment and risk management made an inventory of the risk assessment (RA) and risk management (RM) methods and standards that were known to the working group members. This document is targeted to experts in Information Technology RA/RM, who would like to see and compare properties of RA/RM methods in a concise manner.

In this document, risk assessment / risk management always means Information Technology risk assessment / risk management.

In chapter 2, the WG gives some relevant definitions and draws the scope limits of the inventory.
In chapter 3, it identifies and explains a set of factual attributes to describe essential properties of methods. These attributes make up the template used across this document to describe the considered methods. Then, thirteen RA/RM methods/standards have been described. They are presented in alphabetical order.

As a conclusion, chapter 18 shows a side-by-side comparison of all methods/standards described in this document, based on a limited set of most relevant attributes.

1.2 Working group approach and achievements

The working group's objective was to make an inventory of well-known risk assessment and risk management methods used in Europe. The following approach has been used:

- The identification of the different phases of RA and RM methods, referring on EU and ISO definitions.
- The construction of a limited list of products (methods and standards) dealing with IT related risks.
- The definition of specific attributes to characterise a "product" so as to ease future comparison of products.

Achievements:

- A list of the most relevant RA and RM methods used in Europe.
- A comparison table of RA and RM methods.
- A template that can be used to characterise other RA and RM methods.

2. Introduction

2.1 Introduction

In this document we use the term "**product**", to refer to a published document describing an Information Technology RA/RM method, process or standard.

This document draws up a non-exhaustive list of products, irrespectively of their origin (Europe or not). Nevertheless, only methods that are currently in use within Europe **and** that were known by the WG members have been considered.

The ENISA working group, as a group of independent experts, has defined attributes in order to classify those products 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".

The objective of this document is primarily to present the main characteristics of the products as well as their position in the market.

The last page contains a template that can be filled in and be submitted to the working group, in case that new methods and/or standards may be added to the list.

2.2 Scope limits

Due to the composition of the working group (experts out of 8 EU member states) as well as the limited time available, only a limited number of products were addressed. Therefore, this document will not contain a complete list of methods and standards dealing with IT risks.

Specific products were deliberately excluded from the survey:

- **High-level reference documents**: Documents like the ISO Guide 73 are not taken into consideration.
- **Non-RA/RM products**: Products that are not classified as RA or RM oriented, according to the definitions used in the working group.
- **Unknown methods**: Some methods could not be investigated, because relevant documentation was not available to the members of the working group. An example is Magerit from Spain.
- **General management oriented (i.e. corporate governance) methods**: For example Cobit has been excluded due to this reason.
- **Product security oriented methods**: For example Common Criteria is excluded for this reason.

Software tools[1] were **not** addressed in this survey. Lots of tools exist, commercial tools as well as freeware, and the number of tools is continuously increasing.

[1] A software tool is considered to be a set of programs run by a computer that helps to write documents, or exploit knowledge bases, or give graphical representation, or make computation.

2.3 Remark

This list of attributes is limited to our specific purpose and does not prejudge the quality (i.e. efficiency and effectiveness) of the products. The results are not based on a benchmark but on a WG consensus decision.
It is considered that our focus is IT risks only (including human and physical risk). Hence, a product is considered only if its main focus is IT risk. Otherwise, it will not be mentioned in this paper.

2.4 Definitions

The following EU risk definitions are given in *EU Reg. 2004/460* [2]:

- **Risk assessment:** A scientific and technologically based process consisting of four steps, threat identification, threat characterisation, exposure assessment and risk characterisation

- **Risk management:** The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options.

The definition of risk management as specified by ISO in *ISO/IEC guide73:2002*:

- **Risk management**: Coordinated activities to direct and control an organisation with regard to risk. Note: Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication.

In order to fulfil the objective of the document, we need to have precise attributes to define an RM method. The note from the ISO definition is coherent and compliant with the EU definition and details the different phases of an RM method. Therefore we decided to use those phases to characterise a RM method in this document.

2.5 Acronyms

RA : **R**isk **A**ssessment
RM : **R**isk **M**anagement
SME : **S**mall and **M**edium **E**nterprise
WG : **W**orking **G**roup
IT : **I**nformation **T**echnology

[2] http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_077/l_07720040313en00010011.pdf

3. Explanation of the attributes

3.1 A: Product Identity card

A-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 organisation that provides the product and the country of origin (in case the product originated from a company or national organisation).

A-2: Level of reference of the product
Details about the type of initiator of the product:

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

A-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[3].
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 fulfilment of the phase by the considered product.

A-4: Lifecycle
Date of the first edition, as well as date and number of actual version.

A-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.

A-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.

A-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.

3.2 B: Scope

B-1: Target organisations
Defines the most appropriate type of organisations the product aims at:

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

- **Governments, agencies**: the product is developed by organisations 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.

B-2: Geographical spread

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

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

B-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.

B-4: License and certification scheme

Recognised licensing scheme[4]: there is a recognised scheme for consultants/firms stating their mastering of a method.

Existing certification scheme: an organisation may obtain a certificate, that it has fully and correctly implemented the method on its information systems.

3.3 C: Users viewpoint

C-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.

[4] 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.

C-2: Consultancy support
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).

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

C-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).

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

C-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).

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

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

C-9: Organisational integration
The method provides interfaces to existing processes within the organisation (e.g. project management, procurement, etc.)

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

4. Austrian IT Security Handbook

4.1 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 organisation / association	Public / government organisation
			Austrian federal chancellery

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification	●●	The handbook contains a generic description of RA, but does not specify a special method
Threat characterisation	●	
Exposure assessment	●	
Risk characterisation	●●	

If R.M. method:

R.M. Method phases	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 prototype.
The Austrian IT Security Handbook was originally developed for government organisations, 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 also.

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	GE

7. Price

Free	Not free	Updating fee
X		

4.2 B: Scope

1. Target organisations

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

4.3 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. Organisation processes integration

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

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

5. Cramm

5.1 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 organisation / association	Public / government organisation
			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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	In CRAMM tool
Threat characterisation	●●●	In CRAMM tool
Exposure assessment	●●●	In CRAMM tool
Risk characterisation	●●●	In CRAMM tool

If R.M. method:

R.M. Method phases	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 organisation CCTA (Central Communication and Telecommunication Agency), now renamed into 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 organisations. 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 organisations, 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	

5.2 B: Scope

1. Target organisations

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

5.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

6. Dutch A&K analysis

6.1 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 organisation / association	Public / government organisation
			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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	Handbook, part 2+3
Threat characterisation	●●●	Handbook, part 2+3
Exposure assessment	●●●	Handbook, part 2+3
Risk characterisation	●●●	Handbook, part 2+3

If R.M. method:

R.M. Method phases	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 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 afterwards. Since 1994 the A&K analysis is the only preferred method for risk analysis for Dutch government bodies. Outside 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		

6.2 B: Scope

1. Target organisations

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

6.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

7. Ebios

7.1 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 organisation / association	Public / government organisation
		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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	Section 3, Step 3: study of threat sources, study of vulnerabilities, formalisation of threats, and justification for discarding threats.
Threat characterisation	●●●	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.
Exposure assessment	●●●	Section 3, Step 3, Activity 3.3: threat opportunity Section 4, Step 4, Activity 4.1: risk formulation
Risk characterisation	●●●	Section 3, Step 4, Activity 4.1: risk opportunity, and its consequences (security needs, and impacts)

If R.M. method:

R.M. Method phases	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 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 public as well as private sector, in France and abroad. It is compliant to major IT security standards.

EBIOS gives risk managers a consistent and high-level approach on 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. Thus, it contributes to a relevant communication towards security stakeholders, and spreads security awareness.

EBIOS approach consists in a cycle of 5 phases:

- Phase 1 deals with the 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 then conducted in phases 2 and 3 in a strong dichotomy, yielding an objective vision of their conflict.
- In phases 4 and 5, that 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, their coverage proof is given, 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, GE, ES

7. Price

Free	Not free	Updating fee
X		

7.2 B: Scope

1. Target organisations

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

7.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	Procurement

10. Flexible knowledge databases

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

8. ISF methods for risk assessment and risk management

8.1 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 organisations	International ISF members

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organisation / association	Public / government organisation
		ISF member organisations	

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification	●●● (IRAM, SARA, SPRINT)	
Threat characterisation	●●● (IRAM, SARA, SPRINT)	
Exposure assessment	●●● (IRAM, SARA, FIRM Scorecard)	As a part of the IRAM project in the phase 1 "Business Impact Assessment" SARA, phase 4, step 4.1 "Analyse 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.
Risk characterisation	●●● (IRAM, FIRM Scorecard)	

If R.M. method:

R.M. Method phases	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 organisation 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 enterprise level. It is developed to give a practical approach for monitoring the effectiveness of information security that 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, and 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 that organisations are applying to help them control the business risks associated with their IT-based information systems.

SARA is a detailed methodology for analysing 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 analysing 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 that is better suited to analysing 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 in determining 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 in:

- identifying the vulnerabilities of existing systems and the safeguards needed to protect against them
- defining 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	

8.2 B: Scope

1. Target organisations

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

8.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	Under development

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

9. ISO/IEC IS 13335-2 (ISO/IEC IS 27005)

9.1 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 (organisation based in Switzerland)

2. Level of reference of the product

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

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification	●●	generic: chapter 5.2, examples: annex C
Threat characterisation	●●	generic: chapter 5.2, examples: annex C
Exposure assessment	●●	generic: chapter 5.2, 5.3, examples: annexes C, D
Risk characterisation	●●	generic: chapter 5.2, 5.3, examples: annexes C, D

If R.M. method:

R.M. Method phases	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 for 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	

9.2 B: Scope

1. Target organisations

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

9.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	Yes

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

10. ISO/IEC IS 17799:2005

10.1 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 (organisation based in Switzerland)

2. Level of reference of the product

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

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification	●	Standard is a good practice for initial threat identification indirectly implied.
Threat characterisation	-	Phase not explicitly handled in the document.
Exposure assessment	-	Phase not explicitly handled in the document.
Risk characterisation	-	Phase not explicitly handled in the document.

If R.M. method:

R.M. Method phases	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:

The standard is of UK origin, but adapted to the international needs via ISO. This document shows what should be the 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)	

10.2 B: Scope

1. Target organisations

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

10.3 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. Organisation processes integration

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

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

11. 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 (±2007-2008).

11.1 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 (organisation based in Switzerland)

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organisation / association	Public / government organisation
	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 phases	Included? (-, ●..●●●)	Comments
Threat identification	-	Generic requirement that threat identification has to be made through a recognized method, but no support is provided.
Threat characterisation	-	
Exposure assessment	-	
Risk characterisation	-	

If R.M. method:

R.M. Method phases	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. As being of UK origin, this standard has been adopted by ISO with some modifications. A certificate 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)	

11.2 B: Scope

1. Target organisations

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

11.3 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. Organisation processes integration

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

10. Flexible knowledge databases

Method allows use of sector adapted databases	In commercial tools

12. IT-Grundschutz (IT Baseline Protection Manual)

12.1 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 organisation / association	Public / government organisation
BSI (Germany)			

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat 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.
Threat characterisation	●●●	To each threat, contained in a module, a detailed description of the thread is provided.
Exposure assessment	●●●	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.
Risk characterisation	●●●	Risk characterisation 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 characterisation 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”).

If R.M. method:

R.M. Method phases	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 organisation 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:

- Initialisation of the process:
  - Definition of IT security goals and business environment
  - Establishment of an organisational structure for IT security
  - Provision of necessary resources
- Creation of the IT Security Concept:
  - IT-Structure Analysis
  - Assessment of protection requirements
  - Modelling
  - IT Security Check
  - Supplementary Security Analysis
- Implementation planning and fulfilment
- 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 organisation.

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	GE, EN

7. Price

Free	Not free	Updating fee
X		

12.2 B: Scope

1. Target organisations

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

12.3 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. Organisation processes integration

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

10. Flexible knowledge databases

Method allows use of sector adapted databases	Yes

13. Marion

13.1 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 organisation / association	Public / government organisation
		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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	There is a predefined set of 17 types of threats
Threat characterisation	●●●	Each threat is used against each asset
Exposure assessment	●●●	Step 2 of MARION is the vulnerability assessment
Risk characterisation	●●●	Step 3 of MARION is the risk analysis and the evaluation of the risk

If R.M. method:

R.M. Method phases	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 dates 1998. It is about a methodology of audit, which, as its name indicates it, allows estimating the level of IT security risks of a company through balanced questionnaires giving indicators under the shape of notes in various subjects concurrent in the security. The objective of the method is to obtain a vision of the company audited 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 big subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to assure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is realized to identify the risks (threats and vulnerabilities) that press on 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)	

13.2 B: Scope

1. Target organisations

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

13.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

14. Mehari

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

14.1 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 organisation / association	Public / government organisation
		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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	12 types of scenarios exist (knowledge database)
Threat characterisation	●●●	Each scenario is tested (selection)
Exposure assessment	●●●	To complete the evaluation process of the risk
Risk characterisation	●●●	Final evaluation of impact and potentiality

If R.M. method:

R.M. Method phases	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.
MEHARI proposes an approach for defining risk reduction measures suited to the organisation objectives.
MEHARI provides:

- a risk assessment model
- modular components and processes

MEHARI enhances the ability to:

- find out vulnerabilities through audit
- analyse risk situations

MEHARI includes formulas facilitating:

- threat identification and threat characterisation
- 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)	

14.2 B: Scope

1. Target organisations

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

14.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	No

10. Flexible knowledge databases

Method allows use of sector adapted databases	Corporate data bases

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

15.1 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 organisation / association	Public / government organisation
			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 phases	Included? (-, ●..●●●)	Comments
Threat identification	●●	Criteria only
Threat characterisation	●●	Criteria only
Exposure assessment	●●	Criteria only
Risk characterisation	●●	

If R.M. method:

R.M. Method phases	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[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 organisation assume responsibility for setting the organisation's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organisations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organisation's personnel who gather and analyse information, producing a protection strategy and mitigation plans based on the organisation's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organisation'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		

15.2 B: Scope

1. Target organisations

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

15.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	Information Assurance

10. Flexible knowledge databases

Method allows use of sector adapted databases	No

16. SP800-30 (NIST)

16.1 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 organisation / association	Public / government organisation
NIST (USA)			

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification	●●●	Detailed with samples
Threat characterisation	●●●	Detailed in check-list and with samples
Exposure assessment	-	
Risk characterisation	●●●	Detailed in checklists

If R.M. method:

R.M. Method phases	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		

16.2 B: Scope

1. Target organisations

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

16.3 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. Organisation processes integration

Method provides interfaces to other organisational processes	

10. Flexible knowledge databases

Method allows use of sector adapted databases	

17. Template for new methods

17.1 A: Product identity card

1. General information

Method or tool name	Vendor name	Country of origin

2. Level of reference of the product

National Standardization body	International Standardization body	Private sector organisation / association	Public / government organisation

3. Identification

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

If R.A. method:

R.A. Method phases	Included? (-, ●..●●●)	Comments
Threat identification		
Threat characterisation		
Exposure assessment		
Risk characterisation		

If R.M. method:

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

Brief description of the product:

4. Lifecycle

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

5. Useful links

Official web site	
User group web site	
Relevant web site	

6. Languages

Availability in European languages	

7. Price

Free	Not free	Updating fee

17.2 B: Scope

1. Target organisations

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

2. Geographical spread

Used in EU member states	
Used in non-EU countries	

3. Level of detail

Management		Operational		Technical	

4. License and certification scheme

Recognized licensing scheme	
Existing certification scheme	

17.3 C: Users viewpoint

1. Skills needed

To install	To use	To maintain

2. Consultancy support

Open market	Company specific

3. Regulatory compliance

4. Compliance to IT standards

5. Trial before purchase

CD or download available	Registration required	Trial period

6. Maturity level of the Information system

It is possible to measure the I.S.S. maturity level	

7. Tools supporting the method

Non commercial tools	Commercial tools

8. Technical integration of available tools

Tools can be integrated with other tools	

9. Organisation processes integration

Method provides interfaces to other organisational processes	

10. Flexible knowledge databases

Method allows use of sector adapted databases	

18. List of RA/RM products analysed

The RA/RM products described in the chapters before are shown side-by-side in the table below in order to make comparison possible based on the most relevant attributes.

Attributes / Products	Threat identification	Threat characterisation	Exposure assessment	Risk characterisation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only)	Size of organisation	Skills needed[5]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	●●	●	●	●●	●●●	●●●	●●●	●●●	GE	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, GE, 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, GE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	●●●	●●●	●●●	●●●					EN, FR	Not free	Large	*	N	N	
Mehari	●●●	●●●	●●●	●●●					EN, FR	€100-500	All	**	N	N	RISICARE (ca. € 10.000)
Octave	●●	●●	●●	●●	●●	●●	●●	●●	EN	Free	SME	**	N	N	
SP800-30 (NIST)	●●●	●●●		●●●	●●●	●●●	●●●		EN	Free	All	**	N	N	

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

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