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

30/03/2006

Content

Table of figures

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 the second objective.

1. Introduction

1.1 Why IT security must be managed?

Nowadays, information systems span and pervade more and more enterprise activities. Critical business processes of a company now heavily rely on its information system, in the same way vital functions of a human being rely upon its nervous system. That critical dependency is better perceived when an information system fails fulfilling its function, thwarting thus the vital enterprise processes:

- How much money would you loose in case a hacker or a competitor defaced your website, making your customers wait for 2 day delay to have their order delivered?
- How would your company survive in case a foreign company copied your to-be-patented-but-yet-unprotected new product that has cost you a large amount of research and development effort?
- Would your report on statistics or accountability be trustworthy if your databases were corrupted?
- Would you expect to win a public procurement bid if your commercial proposition was tapped by your main competitor?
- Would you continue to have clients if their home PC crashes down due to a virus whenever they connect to your e-commerce platform?

As a manager, you are already used to manage business risks: financial, operational or social risks. You know how to trade off between stakes, assets, threats, risks and investments. And you know the "PDCA" control loop i.e. Plan the objectives, Do what is planned, Check that it is correctly done, and Act to maintain the objectives. In the same way, managing information risks is a part of your job.

Establishing and maintaining the IT security of your enterprise is a whole process:

- Achieve a relevant, calm and methodical diagnostic of your information system, weighing threats and assets to identify the major risks on your core missions and stakes.
- Implement the necessary and sufficient protective controls, in balance with their operational and economic cost:
  - Applying law and regulation to reduce external risks,
  - Setting up an IT security organization, commensurate to your enterprise,
  - Raising security awareness of your personnel through training and communicating,
  - Implementing technical security controls.
- Check the response accuracy of your IT security through audits.
- React and maintain your information system security to the adequate security level.

1.2 How can the information packages help?

Don't reinvent the wheel! Many risk management methods and best practices already exist. This guide is made for you.

It first helps you to define the profile of your SME with respect of:

- its IT risk exposure,
- the type of its assets,
- its business criticality to IT risks, and
- the resources you can afford.

The information packages then will help you to choose a RA and a RM method through a trade-off fitted in with your security context and commensurate with your resources.

2. IT security risk management is a part of business management

In order to establish risk management, you will need a supporting method. Risk management methods vary from simple step-by-step approaches up to complex methods requiring the support of automated tools.

The first step towards dealing with IT security risk management is to assess the importance of your organisation's information assets. This assessment is done in two steps:

1. Determine the importance of the business processes for the organisation and the environment respectively. This importance may vary from 'high' to 'low':
   - Processes with high importance are the most valuable assets for the organisation (e.g. the production processes) or the environment (e.g. if your organization does air traffic control). Disruption or congestion of such processes results in unacceptable damage[1].
   - Processes with medium importance represent a moderate value for the organisation. Disruption or congestion of such processes results in significant damage.
   - Processes with low importance are of minor value for the organisation. Disruption or congestion of such processes results in minor damage only.
2. Determine the dependency of the business processes on information systems:
   - High dependency. Disruption of information systems results in severe hindering or even congestion of the dependent processes.
   - Medium dependency. Disruption of information system results in significant but not severe hindering of the dependent process.
   - Low dependency. Disruption of information system results in only minor hindering of the dependent process.

Figure 1 below illustrates the criticality as the combination of IT systems dependency and the importance of a business process. This criticality is the major indicator for an IT risk manager to consider the contribution of the IT system to the overall business of the organisation.

For example, a highly important process (e.g. order process) that highly depends upon an IT system (e.g. an electronic form within the Web Portal of the company) must be considered as highly critical by the risk manager (and as such must be subject to risk management).

[1] The term damage should be interpreted broadly (i.e. financial damage, decrease of turnover, deterioration of image, quality reduction, etc).

Importance of process for the business	**Process dependency upon the IT system**		
	Low dependency	***Medium dependency***	***High dependency***
Low importance	no criticality	no criticality	low criticality
Medium importance	no criticality	low criticality	medium criticality
High importance	low criticality	medium criticality	high criticality

Figure 1: Criticality in risk management of an IT system with respect to its contribution to business

The kind of IT security risk management method you need depends on the criticality as illustrated in the cells of the previous table:

Does your organisation have IT systems with medium or high criticality for the business (see corresponding cells in the table)? If so, a risk management based on a formal method is appropriate.

Does your organisation have IT systems only with low criticality for the business (see corresponding cells in the table)? If so, a risk management based on a simple approach is appropriate. Such an approach could be based on widely accepted best practices (e.g. ISO/IEC IS 17799). If necessary, a simple method for risk management or risk analysis can be additionally used.

Does your organisation have IT systems only with no criticality for the business (see corresponding cells in the table)? If so, risk management consists solely of implementing basic security controls (e.g. basic protection). Selection of security controls can be based on best practices.

3. IT security Risk Assessment and Risk Management

As described in chapter 2, IT security risk management is an integral part of a company's management process that deals with the identification, treatment, communication and acceptance of IT security risks. It involves the selection and implementation of countermeasures justified by the identified IT security risks and the reduction of those risks to acceptable levels. It also comprises continuous monitoring of risks and risk communication.

All those steps will be explained in more detail in this chapter and be shown in an example.

A business manager should include IT risk management as one more element in his decision-making.

An IT security risk is composed of an asset, a threat and vulnerability: if one of these items is irrelevant, then there is no risk to encounter. Aggregation of all single IT security risk results in the total IT risk. A key step in the risk management process is risk assessment; this involves evaluating each IT risk as well as the total IT risk, and then giving them priorities.

3.1 Definitions and examples

In this section, we give some simplified definitions[2] and examples limited to the components of IT security risks, namely: asset, threat and vulnerability.

Asset: anything that has value to the organisation (ISO/IEC IS 13335-1).

In our context an asset is a tangible or intangible component of information systems. Assets can be hardware, software, data, buildings, infrastructure, but also products, knowledge resources, customer relationships or reputation. To estimate the risk, firstly the security needs of each asset have to be evaluated by taking into account its value. The asset value could for example be the costs of reconstruction or replacement, or its value for the business functions, the value of lost or destroyed data or property or the value of the lost business opportunity. Determining these values and consequences is called "impact assessment".

Threat: any action or event with the potential to cause harm (based on ISO/IEC IS 13335-1).

Threats can be of different types, for example:

- Environmental (e.g. flood, lightening, storms, earthquakes, etc.)
- Organizational deficits (ill-defined responsibilities, etc.)
- Human errors (wrong e-mail address, missing critical dates, noting passwords on stickers, mistakenly deleting files, etc.)
- Technical failures (hardware failure, short circuits, hard disk crash, etc.)
- Deliberate acts (hacking, phishing, fraud, use of malicious code, theft, etc.)

Sources of threats could be vandalism, espionage or just human mistakes and accidents. In the two first cases the strength of the threat can result from two major factors: the motivation of the threat and the attractiveness of the asset.

Vulnerability: a weakness of an asset that can be exploited by one or more threats (based on ISO/IEC IS 13335-1).

Vulnerabilities can exist in all parts of an IT system, e.g. in hardware or software, in organizational structures, in the infrastructure or in personnel. There are also different types of vulnerabilities, like:

- Physical (no access control, no guards, etc.)
- Logical (no security patch, no anti virus, etc.)

[2] Complete definitions can be found in reference documents [ISO/IEC IS 13335-1] and [EU reg. 2004/460].

- Network (no network segmentation, no security gates, connection to mistrusted parties, etc.)

Typical vulnerabilities resulting from the organizational deficits are, for example, ill-defined responsibilities for information security or the lack of audit trails. Unstable power grids or location in an area susceptible to flood are further examples of vulnerabilities of the environment and infrastructure.

IT security risk: a potential event that a threat will exploit vulnerability in an asset and thereby cause harm to the organization and its business.

3.2 IT Security Risk Assessment

Risk Assessment can be understood as the generation of a snapshot of current risks. More technically, it consists of the following phases:

- Threats identification: identify all relevant threats
- Threat characterization: determine the impact and likelihood of the relevant threats
- Exposure assessment: identify the vulnerability of the assets
- Risk characterization: determine the risks and evaluate their impacts on the business

Complete definitions can be found in document (EU Reg. 2004/460).

Figure 2 below illustrates how IT security risk can be seen as a function of threat, vulnerability and assets value. It also shows that there are different ways to reduce the risks: countermeasures can either reduce the probability for a threat to become true. They can reduce vulnerability or they might help to reduce the impact caused when a threat comes true.

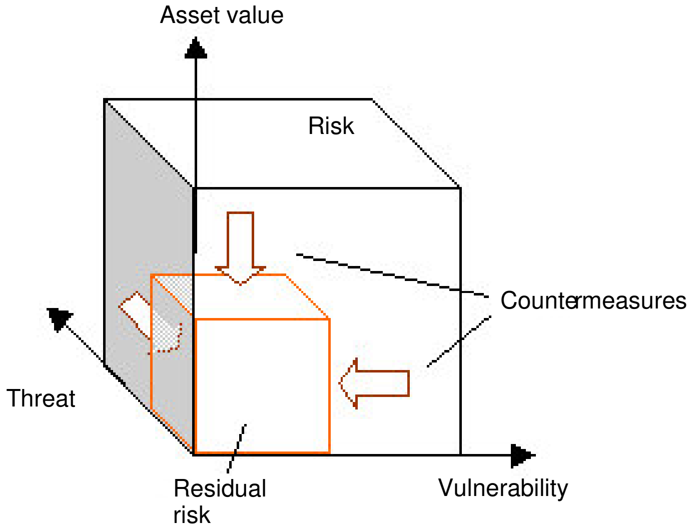

Figure 2: Risk as a function of asset value, threat and vulnerability

Risks that remain after applying countermeasures are called "residual risks". Residual risks have to be considered by the management and be accepted or rejected (in the latter case the risks have to be treated again).

Example

Let us consider the example of a commercial engineer who possesses a company laptop. This hardware stores a copy of the price list of products as well as a database with client data. The commercial engineer is a frequent traveller and he uses his laptop in public places like restaurants or the customers' offices.

In this example:

- **Threats** are the loss or theft of the laptop with the impact of disclosure of company confidential information.
- **Vulnerabilities** result from storing confidential plaintext data on the laptop or leaving the laptop unattended without a screen lock or appropriate password protection.
- **Assets** are the hardware itself (replacement costs in case of theft or loss) and the confidential data for the company. To calculate the value of these assets, several questions have to be answered:
    - What is the cost (money and time) for reconstructing the data in case of loss?
    - What is the degree of confidentiality of the data stored in the laptop?
    - What is the potential impact of data disclosure to competing companies?

Figure 3 shows the phases of the risk assessment process:

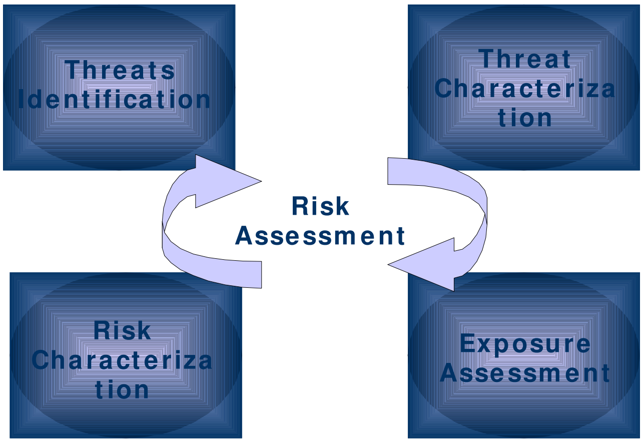

Figure 3: Phases of IT security risk assessment

In the example, as a result of the risk assessment the risk that company information could be disclosed to non-trusted parties has been identified. This risk has major business impacts for the company. Figure 4 below shows the steps required to deal with the risks connected to the threats and vulnerabilities of an asset.

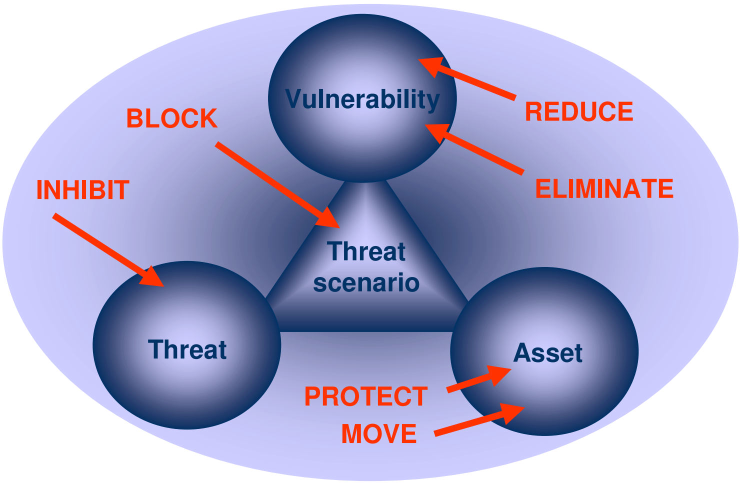

Figure 4: Actions on the components of the risks

3.3 IT Security Risk Management

In order to mitigate the identified IT security risks a risk management process should be implemented. For each assessed risk, the risk manager should propose security controls.

In general, security standards propose security controls categorised in the following areas:

Logical controls (e.g. protection of data, protection of network assets, protection of access to applications etc.)

Physical controls (e.g. alarm systems, fire sensors, physical access control, surveillance etc.)

Organisational controls (e.g. usage rules, administration procedures, process descriptions, definition of roles etc.)

Personnel controls (e.g. sanctions, confidentiality clauses in contracts, training and awareness etc.)

In our example these security controls could be:

- Awareness training for commercial engineers (i.e. control of personnel type)
- Encryption of confidential data stored on the notebook (i.e. control of logical type)
- Only the data actually needed for the trip should be stored on the notebook (i.e. control of organisational type)
- Insurance for the case of theft or loss of the hardware (i.e. control of organisational type)

The security controls should be selected, planned, implemented, communicated and monitored.

IT Security Risk Management is a global approach to risk: on the basis of the assessed risks the process continues with the selection and implementation of security controls ("risk treatment"), the acceptance of risk that cannot or should not be treated further, the communication of risks and their monitoring.

More technically speaking, the process of Risk Management includes:

- **Risk assessment**: find out which risks apply to your business and evaluate them. Management has to decide which risks will be treated or not.

- **Risk treatment**: select and implement security controls to reduce risks. Controls can have different effects, like:
  - mitigation
  - transfer
  - avoidance and
  - retention of risks

  In the example given above, a disk encryption (that would strongly reduce the risk that competing companies get access to confidential data in case the laptop is stolen) is a measure of risk mitigation, an insurance covering the hardware replacement cost is a measure of risk transfer. An example for risk avoidance is to take on the laptop no more than the necessary data.

  You can and should use multiple security controls to treat risks. It is advisable to use different types of controls.

- **Risk acceptance:** Even when the risks have been treated, residual risks will generally remain, even after risk treatment has been performed or if controls are not feasible. The management has to accept the way risks have been treated. Thus, risk acceptance should always be a management decision.

  In our example, applying the four security controls mentioned above reduces the risk considerably, but there is still some residual risk: for example the unavailability of the notebook until it is replaced or the possibility that the encryption system used for disk encryption might be broken. Nevertheless, as in the first instance the possible impact is relatively small, and in the second one the probability that this happens (i.e. that the underlying encryption system is broken) is very small, the risks will probably be accepted.

- **Risk communication:** consists of informing decision makers and involved stakeholders about potential risks and controls. This phase is of high importance and should be integral part of the risk management process. Depending on the involved stakeholders, this communications might be internal or external (e.g. internal units or external partners).

Figure 5 below shows the relation between the different phases of risk management.

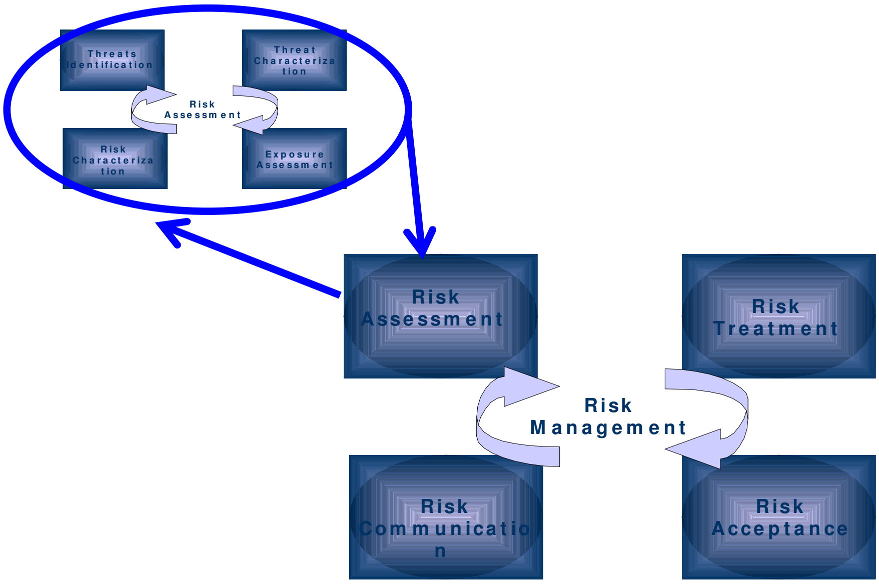

Figure 5: Phases of IT security Risk management

4. Profile for small enterprises with high IT risks

Small sized companies are usually working within a framework where the data-processing environment is standardized but is important for the business. They use packages like off-the-shelf products, having a part or consisting entirely of a “black-box” (with all potential risks associated) and are connected for their business to the Internet, where a lot of IT security threats lurk.

According to their business, SMEs are more or less dependant on their information system. IT companies and cyber shops, for example, offer electronic services to end-users. A quick response to the market needs is certainly of vital importance for their success. The IT system related to this response capability is of major importance for their business process. Tax consultants and lawyers need to use IT applications and IT systems to fulfil their business too. Although loss of confidentiality of their data can have serious legal consequences, the staffs are not in general aware of all details regarding the potential risks.

Even if the staffs of both companies above have special knowledge of information systems, they might not possess special know-how on IT security matters. An aggravating fact is that companies generally do not bear to invest enough resources in IT risk analysis and management.

4.1 Typical Business processes

Some small sized companies may be considered to possess processes that are highly dependent on IT systems, in the sense of chapter 2.

Typical business processes of a small company with high IT risks can be classified in the following categories:

- Production: Processes, necessary for the delivery of the product(s) or service(s) that are actually sold to the customer. (In the most cases, the core business of a company)
- Finance: The internal financial processes (investment, payment)
- Human resources: Processes for the administration of the human resources
- Sales, distribution, marketing: Activities to gain new customers and to keep the already existing ones

The IT security risks considered in this context can arise not only from technical threats but also some from other threats like social engineering, threats associated with the mobility of the used devices, etc.

It is necessary for a company to put a minimum of IT infrastructure in place to ensure the internal communication and the business continuity in the event of disaster (network, backups …). To protect confidential information such companies may need to invest in tools and knowledge for cryptography that may need some specific knowledge.

Often however, the lack of in-house knowledge can make it necessary to outsource these services towards a third party, which can be a big company. In this case it is recommendable to include the adequate insurance clauses regarding IT security risks in the contract. To determine these risks some specific methodology has to be applied.

4.2 Typical IT systems

In the following we will consider small sized companies whose critical business processes have a high IT impact, as described in Figure 1. This is the case for:

Companies working in the IT domain, selling IT products or services (case study 1)

Companies who work with sensitive information, and use information technology for processing this information (case study 2).

4.3 Case SME 1: Online Store

We consider now the special case of an online store selling IT hardware products provided by some partner companies. Figure 6 gives an example of core business processes and their importance for the business:

Business process	**Importance for the business**
Production	High importance
Finance	High importance
Human Resources	Low importance
Marketing	Medium importance

Figure 6: Business processes and their importance for the business, in case SME 1

To carry out these processes, some specific IT systems are needed. The table below (figure 7) assigns the risk management criticality for each IT systems / process, by taking into account their importance and the degree of their dependency (as depicted in figure 1 above).

The last column summarises the criticality with respect to risk management as the maximum of the criticalities found in the same row. This is because the risk management applies on IT systems and not on business processes. For example, as soon as an IT system has high criticality for at least one business process then its overall criticality is high.

IT System	**Business Process**				**Comments**	**Overall criticality** (max. criticality)
	Production: *high importance*	Finance: *high importance*	Human Resources: *low importance*	Marketing: *medium importance*		
Production Web Services: *high dependency*	high criticality				Company sells its products mainly through an online store	high criticality
Production Database: *high dependency*	high criticality				It stores sales data (including personal data)	high criticality
Production File and Print: *medium dependency*	medium criticality				Function needed to process orders, receipts, correspondence with customers	medium criticality

Production / Specific Applications: *high dependency*	high criticality				A set of programs used to access, manage and maintain the production environment	high criticality
Finance and Controlling applications: *low dependency*		low criticality			It stores data to proceed the internal cost-performance ratio	low criticality
Marketing File and Print: *low dependency*				no criticality	It is used by the marketing unit to produce their information material	no criticality
E-Mail: *medium dependency*	medium criticality	medium criticality	No criticality	low criticality	The company has a centralized email-system. This is an indispensable internal and external communication channel	medium criticality
IT-Infrastructure: *high dependency*	high criticality	high criticality	low criticality	medium criticality	Consist of hardware, local network, operating systems, system-software which is needed to operate the information systems	high criticality

Figure 7: Risk management criticality of process / IT systems

4.4 Case SME 2: Law firm

The same approach can be applied in a different business context with the example of a middle sized law firm. In this case, IT-systems are fairly used to store information about the cases, to exchange E-mails and to prepare and process the needed documents. The core processes and their importance for the business are considered in figure 8 below:

Business process	**Importance for the business**
Consultancy	High importance
Case Proceeding	High importance
Finance	Low importance
Human Resources	Medium importance

Figure 8: Business processes and their importance for the business (in case SME 2)

The business process importance and the IT system dependencies according to the content of figure 1 yield the following table. Again, the last column summarises the criticality with respect to risk management as the maximum of the criticalities found in the same row.

IT System	**Business Process**				**Comments**	**Overall criticality** (max. criticality)
	Consultancy: *high importance*	Case Proceeding: *high importance*	Finance: *Low importance*	Human resources: *medium importance*		
Case Proceeding Database: *high dependency*		high criticality			It stores information related to the cases (including personal data)	high criticality
Consulting Database: *high dependency*	high criticality				It stores information related to the clients (including personal data)	high criticality
Finance and Controlling application: *low dependency*			no criticality		It stores data to proceed the internal cost-performance ratio	no criticality
E-Mail: *high dependency*	high criticality	high criticality	low criticality	medium criticality	The company has a centralized email-system. This is an indispensable internal and external communication channel	high criticality

IT-Infrastructure: *high dependency*	high criticality	high criticality	low criticality	medium criticality	Consists of hardware, local network, operating systems, system-software which are needed to operate the information systems	high criticality

Figure 9: Case SME 2: risk management criticality of process / IT systems with regard to their importance / dependency degree

Companies with risk management criticality similar to the above tables need to adequately choose their risk management method.

In case that some of the IT systems described above are outsourced to a third party, the information assessed through the table above is still important. It gives a company the basis to judge the choice of the risk management of its partner. In the respective contractual agreement, the use of the appropriate method has to be clearly specified. Outsourcing risk management is usually the best way to improve security at a reasonable cost.

4.3 RA/RM Methods for SMEs

During the last decade several methods for risk assessment and risk management were developed (s. also inventory of methods in deliverable one). This section provides some assistance for the selection of the most appropriate method for SMEs. Considering the most established methods for risk assessment and risk management in Europe, the ENISA working group characterised them with regard to their features and functions which were judged to be best suited for SMEs. Thus, the selection of the following **methods was based on weighting of the attributes of the template used within deliverable one.**

		Austrian IT Security Handbook	**Dutch A&K Analysis**	**Ebios**	**ISO/IEC IS 13335-2**	**ISO/IEC IS 17799**	**IT-Grund-schutz**	**Mehari**	**Octave**
1	**Is it a risk assessment (RA) and risk management (RM) method?**	RA, RM	RA	RA, RM	RA, RM	RM	RA, RM	RA	RA, RM
2	**Is there an official links**	www.cio.gv.at	No	www.ssi.gouv.fr	www.iso.org	www.iso.org	www.bsi.de/gshb	www.clusif.asso.fr	www.cert.org
3	**Is it available free of charge?**	Yes	Yes	Yes	No	No	Yes	No	Yes
4	**Is it wide-spread?**	Austria	Netherlands	France, Spain, Italy, Belgium, South America,	International standard	International standard	Germany, Austria, Switzerland, Estonia	France French speaking countries	USA
5	**Does it contain information for SMEs?**	Yes	Yes	NA	No	No	Yes	Yes	Yes
6	**Is it possible to apply it without consultancy support[3]?**	Yes	Yes	No	No	Yes	Yes	Yes	Yes
7	**Which regulatory compliance is met?**	NA	VIR	NA	NA	NA	Basel II, KonTraG,	NA	NA
8	**Is it compliant to International IT Standards?**	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA
9	**Is trial before purchase possible?**	Yes	Yes	Yes	No	No	Yes	No	Yes
10	**Are there tools associated with the method?**	Free prototype	Yes Some are free	Yes Free open source software	Yes	Yes	Yes But not free	Yes But not free	Yes But not free
11	**Does the method provide interfaces to other organisational processes?**	Yes	No	Yes	No	Yes	Yes	No	Yes

Figure 10: RA/RM methods for SMEs

[3] All of the above products require a certain level of technical skills to be applied.