Determining Your Organization's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies

Deliverable of the
ENISA 2007-2008 ad hoc Working Group
on
Risk Assessment/Risk Management

Final, v.2.0, September 2008

Table of Contents

1. Executive summary

This paper summarises the work carried out by the ENISA ad hoc working group on risk assessment and management during 2007 to 2008. It aims to provide organizations with a high-level means to sketch their risk profile, defined as the combination of their exposure to threat and vulnerabilities with the potential impact on their critical information assets. Of course, identifying the risk profile through a mere questionnaire should not be confused with the result of a fully conducted risk assessment. This paper also outlines the information risk assessment and management requirements that relate to this profile.

A fully-developed exposure and impact questionnaire is given, mainly based on EBIOS maturity questionnaire [EBIOS]. The analysis of this is described, and results in a risk profile assignment out of a list of 14 profiles. Then, depending on its risk profile, we provide with advice about risk assessment and risk management methods that an organization needs to consider. More detailed recommendations for risk assessment and management requirements are also shown, and related to the deliverables from earlier ENISA working groups on risk assessment and management.

The risk exposure and risk impact analysis is also used to generate processes that enable an organization to consider which information risk assessment and management methodologies are best suited to meet its requirements.

As a result of the work described here, ENISA aims to produce a tool (the Self Assessed Risk Profiler (SARP)) that is able to generate the risk profile for an organization and automatically deliver the appropriate description of its risk assessment and management objectives and relevant charts.

2. Introduction

This document describes the deliverables from the third ENISA working group (WG3) on risk assessment and risk management (RA/RM). Previous working groups have produced deliverables that include a catalogue of published RA/RM items (WG1) and a benchmark methodology for comparing processes, inputs and outputs of RA/RM items (WG2). The deliverables of WG3 draw on the output from both previous WGs.

This document sets out a questionnaire, which is intended to help organizations from any sector or size understand the type of risk management they need and estimate the level of resources they should devote to RA/RM. It shows how this questionnaire can be used to generate the information about an organization’s RA/RM requirements. It also relates the output of the questionnaire to the benchmarking work completed in WG2, thus enabling the organization to select suitable RA/RM items from the catalogue produced by WG1.

An organization’s requirement for RA/RM in its information systems is related to the risks it faces as a result of threats and vulnerabilities, as well as the potential impact of these risks on its information systems. The questions given in section 2 of this document can be used to qualify the requirement of an organization in terms of its risk exposure and potential risk impact.

Section 4 of this document describes how the answers to the questions in section 3 can be analyzed and converted into a profile of the risk exposure and risk impact faced by an organization. Section 5 describes RA/RM requirements appropriate to 14 organizational risk exposure and impact profiles. Section 6 gives the methodology for relating these to the benchmark for RA/RM produced by WG2, thus enabling the selection of RA/RM items as catalogued by WG1, as shown in section 7.4.

3. Exposure and impact qualification

3.1. Scoping the enquiry

Any organization seeking to qualify its potential for information security risk (defined by WG3 as a combination of threat, vulnerability and impact) must be clear about the scope of what they are attempting to qualify. The questions that are outlined in this section are intended as a high level (managerial) assessment and can be answered as they relate to the organization as a whole, or to a part of the organization (such as a single department or business unit). In addition, the individual (or individuals) who answer the questions should have an appropriate level of understanding of the organization – in particular of its business model, its threats and vulnerabilities and the potential for these to affect its business. When answering the questions, respondents are asked to attempt to ignore the effect of any information security controls already in place within their organization.

3.2. Questionnaire

3.2.1. Organization of the questions

WG3 has devised 15 questions about the exposure of the organization to threats and potential sources of vulnerability (referred to as “exposure”) and the potential impact of these (referred to as “impact”) in order to qualify an organization’s requirement for RA/RM. These questions fall into the following sections:

Qualification of exposure:

- As a result of the organization’s business model
- As a result of threats
- As a result of vulnerabilities.

Qualification of impact:

- As a result of the organization’s legal and regulatory requirements
- As a result of its loss of information confidentiality, integrity and availability
- As a result of its use of information systems in support of the business processes.

Nine questions are asked relating to exposure and six relating to impact, making 15 questions in all. All questions offer the responding organization the option of choosing one of four possible answers. Each question is scored depending on the answer given. The questions and choices of answer are listed in the sections below.

3.2.2. Exposure and the organization’s business model

The tables below show two questions that seek to determine the responding organization’s exposure as a result of its business model. The first question probes the likely exposure of the organization by examining its size and use of contractors. The second examines how exposed the organization is as a result of the amount of change and innovation it is involved in. The scores for each question range between 1 and 8.

Question 1: Please choose the statement below which best expresses how large and complex your organization is	**Score**
Small or medium-sized organization, no contractors, or very few, a small number of offices in one country	1
Small medium or large organization, sometimes using contractors, a number of offices in one country	2
Medium to large organization, a number of contractors, offices in more than one country	4
Large or very large organization, many contractors, offices in many countries	8

Question 2: Please choose the statement below which best expresses your organization's attitude to change and innovation	**Score**
Our organization changes slowly and innovation is not a high priority	**1**
Our organization changes to meet market and other requirements and we innovate as necessary	**2**
Our organization embraces change and seeks to innovate wherever possible	**3**
Change and innovation are critical to our organization's business model	**4**

3.2.3. Organization’s exposure to threats

The tables below show three questions that seek to explore the responding organization’s perception of the threats it faces. The first question deals with security incidents, the second with sources of threat (‘threat actors’) and the third with the ability of the threat actors to impact on the organization. The scores for each question range between 1 and 4.

Question 3: To what extent do you consider that non-human factors may cause information security incidents, problems and instabilities in your organization?	**Score**
Very little	**1**
Some	**2**
Potentially significant	**3**
Potentially critical	**4**

Question 4: To what extent do you feel that you have information security incidents, problems and instabilities as a result of human-related incidents from people either within your organization (such as disgruntled employees or employees making mistakes) or outside your organization (such as competitors, criminals, social activists or terrorists)?	**Score**
Very little	**1**
Some	**2**
Potentially significant	**3**
Potentially critical	**4**

Question 5: Do you think that the people either within or outside your organization, who may have the motivation to cause incidents, problems and instabilities, are likely to be knowledgeable and have the resources to attack you?	**Score**
Unlikely to be knowledgeable and have effective resources	**1**
May have knowledge and effective resources	**2**
Likely to have knowledge and effective resources	**3**
Certain to have knowledge and effective resources	**4**

3.2.4. Exposure to organizational vulnerabilities

The tables below show four questions that explore some organizational vulnerabilities. The first question explores the vulnerability of the IT systems as a result of their complexity (and consequent problems of support). The second question considers use of the Internet to connect to customers and third parties. The third considers access to your IT systems and networks by business partners (such as outsourced suppliers). The fourth question considers the issue of home and remote working. Scoring for the questions ranges from 1 to 4.

Question 6: Which of the statements below best describes the complexity of your IT resources (e.g. number of different applications, systems and legacy software)?	Score
Little complexity	1
Some complexity, but no legacy systems	2
Some complexity	3
Much complexity	4

Question 7: Which of the statements below best describes your use of the Internet both internally and to interact with customers and third parties?	Score
Internet usage is insignificant (e.g. for information purposes only)	1
Internet usage is useful to our business (e.g. for transactional purposes)	2
Internet usage is important to our business (we can survive without it)	3
Internet usage is business critical (we can’t survive without it)	4

Question 8: Which of the statements below best describes the access that partners (e.g outsourced service providers) have to your organization's IT networks and resources?	Score
No access	1
Some access, but restricted and not important to the business	2
Access is not widely used, but is important	3
Access is widely used and/or business critical	4

Question 9: Which of the statements below best describes home working and remote working in your organization?	Score
No home or remote working	1
We have a small number of home and remote workers	2
Most of our employees and contractors sometimes work remotely or from home	3
Home and remote working is an integral and important part of our business model	4

3.2.5. Impact of legal and regulatory issues

The question below explores the potential impact on the responding organization's information security of its requirement for legal and regulatory compliance and oversight. This question is considered to be so important that the scoring for this question ranges from 1 to 8.

Question 10: How strongly is your business affected by legal and regulatory requirements and the possible breach of these?	Score
Not very	1
Somewhat	2
Significantly	4
Critically	8

3.2.6. Impact from information loss

The tables below show three questions that explore potential impact on the responding organization of loss of business-critical information held on information systems. The first question explores the consequence of lost availability, the second of lost integrity and the third of compromised confidentiality. The scores for each question range between 1 and 4.

Question 11: What would the likely impact on your organization be of your inability to access business critical information from your information systems?	Score
Little impact	1
Significant impact	2
Severe impact	3
Critical impact, including breakdown of the organization	4

Question 12: What would the likely impact on your organization be if changes were made to business critical information on your information systems without your knowledge or authorisation?	Score
Little impact	1
Significant impact	2
Severe impact	3
Critical impact, including breakdown of the organization	4

Question 13: What would the likely impact on your organization be if the confidentiality of the business critical information on your information systems was compromised?	Score
Little impact	1
Significant impact	2
Severe impact	3
Critical impact, including breakdown of the organization	4

3.2.7. Impact from organization's information systems

The tables below show two questions that explore the potential impact on the responding organization as a result of its use of information systems. The first question explores the importance of information systems to the overall business of the organization, querying the potential impact of a disaster affecting these systems on the organization itself. The second question looks at the impact this would have on the organization's business partners and other stakeholders. The scores for each question range between 1 and 8.

Question 14: How significant are your organization's information systems in enabling you to achieve your business objectives?	Score
Incidental to our objectives	1
Useful in achieving our objectives	2
Very valuable in helping us to achieve our objectives	4
Critical to enabling us achieve our objectives	8

Question 15: What would the impact be on your business partners, customers and external stakeholders of a disaster to your information systems?	Score
Negligible or small	1
Significant	2
Very significant	4
Would cause severe damage	8

4. Analysis of the answers

Interaction between an organization's exposure and the potential impact this might have, gives a measure of the organization's requirement for RA/RM. Analysis of the answers to the questions shown in section 3 can be carried out by totaling the scores for the elements of exposure (business model, threats and vulnerabilities) and the elements of impact (legal and regulatory, information loss and information systems).

Plotting the results on a simple *xy* chart will give a preliminary indication of the organization's exposure and impact. Figure 1 is an example of such a chart, divided into four quadrants, labeled "low exposure, low impact", "high exposure, low impact", "low exposure, high impact" and "high exposure, high impact".

Figure 1 shows the results from the completion of a questionnaire by an example organization (ENISA). The intersection between threat and vulnerability and impact for that organization is indicated in figure 1 by the red diamond. This is located in the "low exposure, high impact" quadrant of the chart. Organizations of this type must be vigilant in the management of their information risks, because the impact on them is potentially high. However, because their threat and vulnerability exposure is relatively low, their assessment need not be intensive and their management controls need not be highly targeted.

This is in contrast to an organization in the upper left quadrant, where a high threat and vulnerability exposure but low potential impact implies the need for sophisticated risk assessment in order to determine those assets that are at critical risk, and therefore require most protection. The application of targeted controls in such cases will ensure that resources are not wasted in protecting assets whose loss or damage would have a low impact on the business.

It will be evident that organizations in the upper right quadrant will need to deploy more mature and complete RA/RM methodologies. Those in the lower left quadrant, on the other hand, will be most effectively served by using RA/RM methodologies that can be simply and quickly deployed and will use minimum appropriate resources.

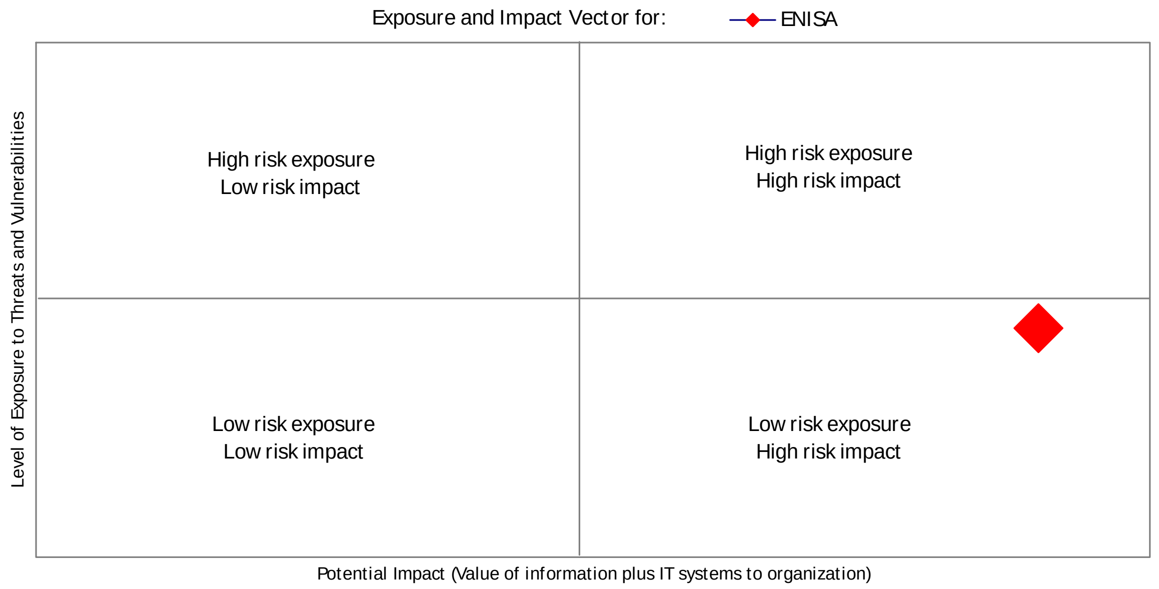


Figure 1: Threat, vulnerability and impact plot for the example organization

It will therefore be appreciated that the qualification questions in section 2 will enable an organization to easily determine the fundamental nature of its RA/RM requirements. It must be noted, however, that this process is not intended as a substitute for a risk assessment; indeed it is geared towards indicating what the risk assessment and management requirements of the organization are. The methodology for determining this is discussed in the next section.

5. Linking exposure and impact to RA/RM requirements

5.1. Granularity of RA/RM requirements

As a first step towards determining risk assessment and management requirements, more granularity is needed than is shown in figure 1. Each of the main quadrants of the chart in figure 1 is therefore further sub-divided. In figure 2, these sub-divisions are shown in tabular form and characterized as being "low", "some", "significant" or "critical" for both exposure (y-axis) and impact (x-axis). It should be noted that, after consideration of a number of actual organizations, WG3 has concluded that organizations expecting a low impact are unlikely to have significant or critical exposure. As can be seen in figure 2, therefore, these two possibilities have been ignored (greyed out). There are therefore a total of 14 segments, not 16. These segments are numbered from 1 to 14 in figure 2. This table is repeated in diagrammatic form throughout the descriptions which follow, for guidance purposes.

Exposure to threats and vulnerabilities	**Critical**		**6**	**10**	**14**
	Significant		**5**	**9**	**13**
	Some	**2**	**4**	**8**	**12**
	Low	**1**	**3**	**7**	**11**
		Low	**Some**	**Significant**	**Critical**
		Impact of exposure to threats and vulnerabilities			

Figure 2: More granular exposure and impact assessment

5.2. Description of the requirements

In order to link the outcome of the questionnaire outlined in section 3 with the organization's requirements for risk assessment and management, WG3 has used the methodology that was devised by WG2 to characterise the following 15 RA/RM processes:

- P.1 Definition of external environment
- P.2 Definition of internal environment
- P.3 Generation of risk management context
- P.4 Formulation of impact limit criteria
- P.5 Identification of risks
- P.6 Analysis of relevant risks
- P.7 Evaluation of risks
- P.8 Identification of options
- P.9 Development of action plan
- P.10 Approval of action plan
- P.11 Implementation of action plan
- P.12 Identification of residual risks
- P.13 Risk acceptance
- P.14 Risk indicator gathering and reporting
- P.15 Risk communication, awareness and consulting

WG2 identified a number of inputs and outputs to and from each of these processes. On the basis of these, descriptions characterising the risk assessment and management objectives for each of the 14 segments have been drawn up by WG3. These descriptions are listed below.

Note: in these descriptions the term "information risk" is used to denote the outcome of a threat exploiting a vulnerability or weakness to have an impact on business critical information assets.

1. Low exposure, low impact.

General information:

- Organizations in this situation require little investment in either human or material resources for information risk management purposes.
- If your organization is of this type, you need to understand the threats to your information, the possible impacts on it and have a simple and informal plan for how you will deal with those threats and impacts.

Level of concern:

- Only some processes need to be considered, and at a basic level.

- Your focus should be on information risk treatment.

Requirements:

- Understanding your market, financial, political, social and cultural context.
- Understanding your legal and regulatory requirements.
- Understanding your external stakeholders (customers, partners etc.)

Recommendations:

- Use easily available, basic guides to good practice and simple checklists.
- Generate a short list of information risk management options and use this as your plan.

2. Some exposure, low impact

General information:

- Organizations in this situation require a small investment in human and material resources for information risk management purposes, as a result of their exposure to some threats and vulnerabilities.
- If your organization is of this type you need to develop a basic understanding of your requirements for information, how you use it and the risks to it.

Level of concern:

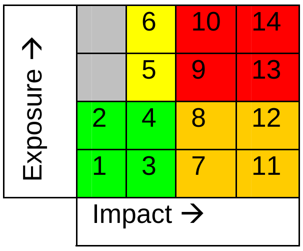
- A few processes need to be considered at a basic level.
- Your focus should be on information risk treatment.

Requirements:

- Understanding your information assets (e.g. people and systems) and processes.
- Understanding your internal stakeholders and organization.
- Understanding your risk appetite, risk acceptability and strategy for managing this.
- Identifying all your strategies (e.g. business strategy, overall IT strategy) potentially relevant to information risk.
- Understanding the threats to your information and the possible impacts on it.
- Having a simple and informal plan for how you will deal with those threats and impacts.

Recommendations:

- Use easily available, basic guides to good practice and simple checklists that will allow you to perform some basic reporting.
- Coordinate and cost the actions to be taken to control your threats and impacts.
- Prioritize the actions to be taken..
- Assign responsibility for carrying out those actions.
- Provide basic reporting on how the actions are carried out.



Exposure ↑	▨	🟨 6	🟥 10	🟥 14
	▨	🟨 5	🟥 9	🟥 13
	🟩 2	🟩 4	🟧 8	🟧 12
	🟩 1	🟩 3	🟧 7	🟧 11
	Impact →			

3. Low exposure, some impact

General information:

- Organizations in this situation require a basic understanding of the context in which their business works.
- If your organization is of this type you need to develop a general understanding of the legal and regulatory aspects of your business and the inter-relationship between information risk and your business's strategic programs.

Level of concern:

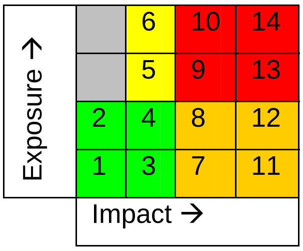
- Basic information risk analysis should be used
- Information risk treatment is essential.

Requirements:

- Understanding which of your information assets need to be protected.
- Understanding the threats to your information assets, the possible impacts on your business if those assets are not available, or if their confidentiality or integrity are compromised.
- Scoping and planning how you deal with the outcome of threats and impacts.
- Defining who needs to be involved in assessment and management of threats and impacts.
- Having a simple and informal plan for how you will deal with those threats and impacts.

Recommendations:

- Use easily available, basic guides to good practice and simple checklists that will allow you to perform some basic reporting.
- Coordinate and cost the actions to be taken to control your threats and impacts.
- Prioritize the actions to be taken..
- Assign responsibility for carrying out those actions.
- Provide basic reporting on how the actions are carried out.



Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

4. Some exposure, some impact

General information:

- Organizations of this type may encounter some problems, but these are not likely to be critical to their business.
- If your organization is of this type, you should understand the information risk to your business and have a regular means of reviewing this.

Level of concern:

- Basic to intermediate analysis of information threats and impacts should be carried out
- Appropriate information risk treatment is essential.

Requirements:

- Understanding what level of protection your information needs by classifying it according to the damage that could be done to your business if it were not available, or if its confidentiality or integrity were to be compromised.
- Defining a regular assessment regime for information risk management.
- Prioritize the actions you will take to manage information risk.

Recommendations:

- Have a basic understanding of the context in which your business works, including legal and regulatory aspects and your interactions with customers, partners etc.
- Develop a basic understanding of your requirements for information, how you use it and the importance of it to your business; giving it a simple classification according to the level of protection it needs.
- Responsibility for carrying out those actions should be assigned, approved, coordinated and costed.
- Ensure that you produce basic internal reports on how the actions have been carried out and their effectiveness, and these reports should trigger reconsideration of the threats and impacts.
- Provide your employees with basic training and awareness in information risk and its management.

5. Significant risk exposure, some risk impact

General information:

- Organizations of this type need to be concerned about their information risk.
- If your organization is of this type, you need dedicated resources to manage your information risks.

Level of concern:

- Information risk analysis is necessary.
- You must have a clearly defined information risk management method.
- You must carry out information risk treatment.

Requirements:

- Understanding threats to your information, its vulnerabilities and the potential impact on your business.
- Using external information sources, checklists, methods and tools to help you understand threats to your information and the potential impact on your business.
- Defining decision and reasoning for disregarding certain threats, and vulnerabilities.

Recommendations:

- Produce a detailed plan identifying controls and how you will implement them. Responsibility for carrying out the plan should be formally assigned, approved and costed.
- Some basic information about the cost effectiveness of these actions should be included in the report as well.
- Have a clear understanding of the context in which your business works, including legal and regulatory aspects and your interactions with customers, partners etc., and the inter-relationship between information risk and all the strategic programs of your business.
- Develop a detailed program to understand your requirements for information, how you use it and the importance of it to your business; giving it a formal classification according to the level of protection it needs.
- Decide about which threats, vulnerabilities and impacts must be controlled and which can be ignored.
- Align identified threats and vulnerabilities with the impact these might have on your classified information assets and record this formally.
- The plan should be coordinated to a basic extent with other strategic actions you are carrying out. You should ensure that you produce clear and detailed internal reports on how the actions have been carried out, their effectiveness and the level of risk that is likely to remain after controls have been implemented.
- The reports should trigger formal reconsideration of the threats and impacts on a regular basis. You should provide your employees with basic training and awareness in information risk.

Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

6. Critical exposure, some impact

General information:

- Organizations of this type need to be concerned about their information risk.
- If your organization is of this type, you need dedicated resources, able to take strong measures to protect you from potential threats and vulnerabilities.

Level of concern:

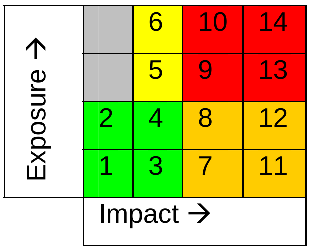
- Information risk analysis is essential.
- You must have a clearly defined information risk management method.
- You must carry out information risk treatment.

Requirements:

- Listing threats, impact, existing controls and related vulnerabilities in relation to the sensitivity of your information.
- Listing quantified risks in relation to the sensitivity of your information.
- You will need to gain some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled, so to have a clear and detailed understanding of the threats to your information assets that can impact your business.
- Develop a basic understanding of the inter-relationship between information risk and all the strategic programs of your business, and to define to a basic extent your risk appetite, risk acceptability and strategy for managing this.

Recommendations:

- The plan should be clearly and effectively coordinated with other strategic actions you are carrying out.
- The reports should trigger formal reconsideration of the threats and impacts.
- Develop a detailed program to understand your requirements for information, how you use it and the importance of it to your business; giving it a formal classification according to the level of protection it needs.
- Produce a very detailed action plan identifying the available options to control risks and how you will implement them in order of priority.
- Responsibility for carrying out the plan should be formally assigned, communicated, approved and costed.
- Ensure that you produce clear and detailed internal reports on how the actions have been carried out, their effectiveness, and very detailed information on the risks that is likely to remain after controls have been implemented.
- Some basic information about the cost effectiveness of these actions should be included in the report as well.
- Provide your employees with basic training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.
- Make detailed formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored and record this formally.
- Have a basic understanding of the context in which your business works, with a clear and detailed view of legal and regulatory aspects and of your interactions with customers, partners and all internal and external stakeholders.



Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

7. Low risk exposure, significant risk impact

General information:

- Organizations of this type have a relatively small degree of exposure (perhaps through limited use of the Internet) but deal with information that is significant to their business.
- If your organization is of this type, you must ensure that you understand the information risk and your information risk treatment plan should be carefully targeted.

Level of concern:

- Appropriate information risk assessment should be carried out to an intermediate level
- Targeted risk treatment is essential.

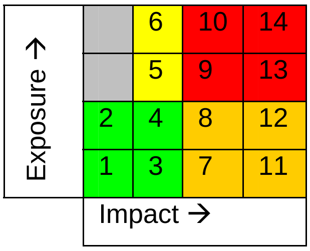
Requirements:

- Recording formal decisions and agreements about the risks you will manage.
- Understand your requirements for information, how you use it, the threats to it and the possible impacts on your business; giving it a simple classification according to the level of protection it needs.

- Prioritize the actions you will take to control the threats and impacts to your information assets and assign responsibility for carrying them out.
- Actions need to be coordinated and costed and you should ensure that you provide some basic reports on how they are carried out.
- Assign responsibility and resources for carrying out those actions and you need to provide some basic reports on how they are carried out and their effectiveness and the level of risk that is likely to remain after controls have been implemented.

Recommendations:

- Produce a basic plan identifying controls and how you will implement them.
- Have a basic understanding of the context in which your business works, including legal and regulatory aspects and the inter-relationship between information risk and all the strategic programmes of your business.
- The reports should trigger reconsideration of the threats and impacts.



Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

8. Some risk exposure, significant risk impact

General information:

- Organizations of this type have some degree of exposure and deal with information that is significant to their business.
- If your organization is of this type, you must ensure that you have a good understanding of the information risk and your information risk treatment plan should be carefully planned and targeted.

Level of concern:

- Good, basic information risk assessment should be used.
- Good, basic information risk treatment must be used.

Requirements:

- Generate list of risk management options.
- Gain some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled.

Recommendations:

- Have a basic understanding of the context in which your business works, including legal and regulatory aspects and your interactions with customers, partners etc.
- Develop a basic understanding of your requirements for information, how you use it and the importance of it to your business; giving it a simple classification according to the level of protection it needs.
- Make formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored.
- Align identified threats and vulnerabilities with the impact these might have on your classified information assets.
- Produce a clear and detailed plan identifying controls and how you will implement them.
- Responsibility for carrying out that plan should be assigned, approved and costed.
- The plan should be coordinated to a basic extent with other strategic actions you are carrying out.

- Ensure that you produce basic internal reports on how the actions have been carried out, their effectiveness, cost and the level of risk that is likely to remain after controls have been implemented.
- The reports should trigger reconsideration of the threats and impacts.
- provide your employees with basic training and awareness in information risk

9. Significant risk exposure, significant risk impact

General information:

- Organizations of this type face more complex challenges and consequently require more complex solutions
- If your organization is of this type, you must ensure that all parts of information risk assessment and management are considered.

Level of concern:

- Intermediate level attention to all aspects of information risk assessment.
- Intermediate level attention to all aspects of information risk treatment.

Requirements:

- Assignment of responsibility for carrying out your risk management activities.
- Defining your prioritized risk management action plan and allocating resources
- Develop a clear and detailed understanding of the inter-relationship between information risk and all the strategic programs of your business. To deal with IT risks more effectively, you should develop a precise understanding of your risk appetite, risk acceptability and strategy for managing this.
- Gain some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled, so to have a deep understanding of the threats to your information assets that can impact your business.

Recommendations:

- Have a good understanding of the context in which your business works, including legal and regulatory aspects and a clear understanding of your interactions with customers, partners and all internal and external stakeholders.
- Develop a detailed program to understand your requirements for information, how you use it and the importance of it to your business; giving it a full-fledged formal classification according to the level of protection it needs.
- Make detailed formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored and record this formally.
- Produce a very detailed action plan identifying the available options to control risks and how you will implement them in order of priority.
- Responsibility for carrying out the plan should be formally assigned, communicated, approved and costed.
- The plan should be clearly and effectively coordinated with other strategic actions you are carrying out.
- Ensure that you produce very extensive internal reports on how the actions have been carried out, their effectiveness, and very detailed information on the risks that is likely to remain after controls have been implemented.
- Some basic information about the cost effectiveness of these actions should be included in the report as well. The reports should trigger formal reconsideration of the threats and impacts on a regular basis.
- Provide your employees with an extensive training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.

Exposure ↑		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

10. Critical risk exposure, significant risk impact

General information*:*

- Organizations of this type face complex challenges and consequently require complex solutions
- If your organization is of this type, you must ensure that all parts of information risk assessment and management are considered, with more emphasis on understanding your information risks because of your critical risk exposure.

Level of concern:

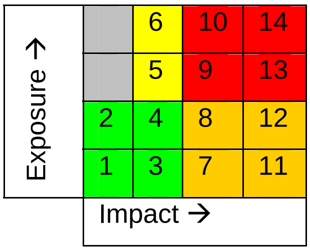
- Information risk assessment is essential.
- Information risk management is essential.

Requirements:

- Defining and approving action plan reports and lists of activities to be undertaken*.*
- You also need to develop a clear and detailed understanding of the inter-relationship between information risk and all the strategic programs of your business.
- Gaining information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled, so to have a deep understanding of the threats to your information assets that can impact your business.

Recommendations:

- Have a basic understanding of the context in which your business works, with a very detailed view of legal and regulatory aspects and a clear understanding of your interactions with customers, partners and all internal and external stakeholders.
- To deal with IT risks more effectively, you should develop a clear understanding of your risk appetite, risk acceptability and strategy for managing this.
- Develop a very detailed program to understand your requirements for information, how you use it and the importance of it to your business; giving it a full-fledged formal classification according to the level of protection it needs.
- Make detailed formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored and record this formally.
- Produce a very detailed action plan identifying the available options to control risks and how you will implement them in order of priority.
- Responsibility for carrying out the plan should be formally assigned, communicated, approved and costed.
- The plan should be clearly and effectively coordinated with other strategic actions you are carrying out.
- Ensure that you produce very extensive internal reports on how the actions have been carried out, their effectiveness, and very detailed information on the risks that is likely to remain after controls have been implemented.
- Some basic information about the cost effectiveness of these actions should be included in the report as well.
- The reports should trigger formal reconsideration of the threats and impacts
- Provide your employees with an extensive training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.



Exposure ↑		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

11. Low risk exposure, critical risk impact

General information:

- Organizations of this type are less exposed to information risk, however, if a problem occurs there will be critical impacts on the business, which could result in very significant damage.
- If your organization is of this type, you should concentrate on ensuring that your critical information assets are well protected.

Level of concern:

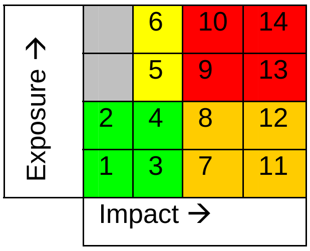
- Information risk assessment must be used to identify those assets that are business critical.
- Information risk management should be concentrated on those assets identified as critical.

Requirements:

- Implementing risk management activities and coordinating these with other relevant projects (e.g. IT system updates, business continuity planning).
- Assigning risk management activities and reporting on implementation and costs
- Understand your requirements for information, how you use it, the threats to it and the possible impacts on your business; giving it a simple classification according to the level of protection it needs.
- Prioritize the actions you will take to control the threats and impacts to your information assets and assign responsibility for carrying them out.
- Those actions will need to be coordinated and costed and you should ensure that you provide some basic reports on how they are carried out.
- Assign responsibility and resources for carrying out those actions and you need to provide some basic reports on how they are carried out and their effectiveness and the level of risk that is likely to remain after controls have been implemented.

Recommendations*:*

- You should have a basic understanding of the context in which your business works, including legal and regulatory aspects and your interactions with customers, partners etc., and the inter-relationship between information risk and all the strategic programmes of your business
- decide about which threats, vulnerabilities and impacts must be controlled and which can be ignored
- Produce a basic plan identifying controls and how you will implement them.
- The reports should trigger reconsideration of the threats and impacts.
- provide your employees with basic training and awareness in information risk.



Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

12. Some risk exposure, critical risk impact

General information:

- Organizations of this type are somewhat exposed to information risk, and if a problem occurs there will be critical impacts on the business, which could result in very significant damage.
- If your organization is of this type, you should have some appreciation of potential information risks, but concentrate on ensuring that your critical information assets are well protected.

Level of concern:

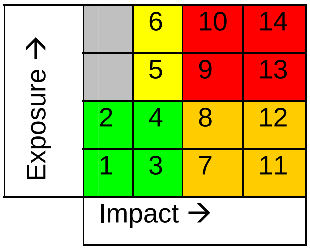
- Information risk assessment must be performed to a more advanced level.
- Information risk treatment is essential for business critical information assets.

Requirements:

- Understanding residual risks (those left after controls have been implemented).
- Triggering iteration of threat and vulnerability assessment and decision activities.
- Gain some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled.

Recommendations:

- You should have a basic understanding of the context in which your business works, including legal and regulatory aspects and your interactions with customers, partners etc., and the inter-relationship between information risk and all the strategic programmes of your business.
- Develop a detailed programme to understand your requirements for information, how you use it and the importance of it to your business; giving it a formal classification according to the level of protection it needs.
- Decide about which threats, vulnerabilities and impacts must be controlled and which can be ignored.
- Align identified threats and vulnerabilities with the impact these might have on your classified information assets and record this formally.
- Produce a clear and detailed plan identifying controls and how you will implement them.
- Responsibility for carrying out the plan should be formally assigned, approved and costed.
- The plan should be coordinated to a basic extent with other strategic actions you are carrying out.
- Ensure that you produce clear and detailed internal reports on how the actions have been carried out, their effectiveness and the level of risk that is likely to remain after controls have been implemented.
- Some basic information about the cost effectiveness of these actions should be included in the report as well.
- The reports should trigger formal reconsideration of the threats and impacts.
- Provide your employees with basic training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.



Exposure →		6	10	14
		5	9	13
	2	4	8	12
	1	3	7	11
	Impact →			

13. Significant risk exposure, critical risk impact

General information:

- Organizations of this type are both exposed to information risk, and have the potential to suffer critical impacts on the business, which could result in very significant damage.
- If your organization is of this type, you should have good appreciation of potential information risks and also ensure that your critical information assets are well protected.

Level of concern:

- Advanced information risk assessment must be deployed.
- Advanced information risk management methods must be implemented.

Requirements:

- Deciding on how effectively risks have been managed and documenting this.
- You also need to develop a clear and detailed understanding of the inter-relationship between information risk and all the strategic programmes of your business
- Gaining some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled, so as to have a deep understanding of the threats to your information assets that can impact your business.

Recommendations:

- Use of common/basic literature and good usage practice
- You should have a clear and detailed understanding of the context in which your business works, of your interactions with customers, partners and all internal and external stakeholders and a very detailed view of legal and regulatory aspects that affect your business.
- To deal with IT risks more effectively, you should develop a clear understanding of your risk appetite, risk acceptability and strategy for managing this.

- Develop a very detailed programme to understand your requirements for information, how you use it and the importance of it to your business; giving it a full-fledged formal classification according to the level of protection it needs.
- Make very detailed formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored and record this formally.
- Produce a very detailed action plan identifying the available options to control risks and how you will implement them in order of priority.
- Responsibility for carrying out the plan should be formally assigned, communicated, approved and costed.
- The plan should be clearly and effectively coordinated with other strategic actions you are carrying out.
- Ensure that you produce very extensive internal reports on how the actions have been carried out, their effectiveness, and very detailed information on the risks that is likely to remain after controls have been implemented.
- Detailed information about the cost effectiveness of these actions should be included in the report as well.
- The reports should trigger formal reconsideration of the threats and impacts.
- Provide your employees with an extensive training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.

14. Critical risk exposure, critical risk impact

General information:

- Organizations of this type are probably large, global enterprises or large government departments which are both exposed to critical information risk, and have the potential to suffer critical impacts on their business.
- If your organization is of this type, you must have an advanced understanding of potential information risks and also ensure that your critical information assets are well protected.

Level of concern:

- All stages of information risk assessment and management must be deployed and implemented at an advanced level.

Requirements:

- Internal reporting on your management of risks and incidents.
- External reporting on your management of risks and incidents.
- Reporting on the cost effectiveness of your risk management.
- Gaining some basic information from a number of sources (such as checklists, standards and reports) about threats, vulnerabilities and impacts on your information, and how these can be controlled, so to have a deep understanding of the threats to your information assets that can impact your business.
- Developing a clear and detailed understanding of the inter-relationship between information risk and all the strategic programmes of your business.

Recommendations:

- You should have a clear and detailed understanding of the context in which your business works, of your interactions with customers, partners and all internal and external stakeholders and a very detailed view of legal and regulatory aspects that affect your business.
- To deal with IT risks more effectively, you should develop a clear understanding of your risk appetite, risk acceptability and strategy for managing this.
- Develop a very detailed programme to understand your requirements for information, how you use it and the importance of it to your business; giving it a full-fledged formal classification according to the level of protection it needs.
- Make very detailed formal decisions about which threats, vulnerabilities and impacts must be controlled and which can be ignored and record this formally.
- Produce a very detailed action plan identifying the available options to control risks and how you will implement them in order of priority.
- Responsibility for carrying out the plan should be formally assigned, communicated, approved and costed.
- The plan should be clearly and effectively coordinated with other strategic actions you are carrying out.

- Ensure that you produce very extensive internal reports on how the actions have been carried out, their effectiveness, and very detailed information on the risks that is likely to remain after controls have been implemented.
- Detailed information about the cost effectiveness of these actions should be included in the report as well.
- The reports should trigger formal reconsideration of the threats and impacts. You should provide your employees with an extensive training and awareness in information risk and produce a simple communication plan about your information risk management for stakeholders in your business.

5.3. Detailed objectives

WG3 has also produced a table detailing the objectives that organizations in each of the 14 segments might have for each of the 15 RA/RM process as identified by WG2 (see the previous section). In table 1 (below) the objectives within each process are shown as follows:

- **0:** Not Required – the process is not needed by an organization of this type
- **1:** Basic – a simple and informal process is needed
- **2:** Intermediate – a formal and documented process is needed
- **3:** Advanced – a detailed process is required with full documentation and auditing.

Table 1 shows these objectives (labelled “0” to “3”) for each of the 14 segments (numbered 1 to 14 as in the previous section), as determined by the exposure and impact qualification questionnaire described in section 2.

Process	**Process objectives**	**Level needed for each of the 14 segments in figure 2**													
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
1	Understanding your market, financial, political, social and cultural context	0	0	0	1	0	1	1	1	1	2	2	2	2	2
	Understanding your legal and regulatory requirements	0	0	1	1	1	1	1	1	2	2	3	3	3	3
	Understanding your external stakeholders (customers, partners etc.)	0	0	0	1	0	1	1	1	2	2	2	2	2	2
2	Understanding your information assets (e.g. people and systems) and processes	1	1	1	1	1	1	1	1	1	2	2	2	3	3
	Understanding your internal stakeholders and organization	1	1	1	1	1	1	1	1	2	2	2	2	3	3
	Understanding your risk appetite, risk acceptability and strategy for managing this	1	1	1	1	1	1	1	1	2	2	3	3	3	3
	Identifying all your strategies (e.g. business strategy, overall IT strategy) potentially relevant to information risk	1	1	1	1	1	1	1	1	2	2	3	3	3	3
3	Understanding which of your information assets need to be protected	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	Scoping and planning how you deal with risk (e.g. assessing risk and taking appropriate action)	1	1	1	1	1	1	1	2	2	2	2	2	2	2
	Defining who needs to be involved in assessment and management of risk	0	0	0	0	0	1	1	1	1	2	2	2	2	2
4	Understanding what level of protection your information needs (classifying your information)	0	0	0	1	1	1	1	2	2	2	2	3	3	3
	Defining a regular assessment regime for your information risk	0	0	0	0	0	0	1	1	1	1	2	2	2	2
5	Understanding threats to your information and the potential impact on your business	1	1	1	1	1	1	1	2	1	2	2	2	3	3
	Using external information sources, checklists and tools to help you understand threats to your information and the potential impact on your business	0	0	0	0	0	0	0	1	1	1	1	1	1	2
	Defining decision and reasoning for disregarding certain threats, and vulnerabilities	0	0	0	0	0	1	1	1	1	1	2	2	2	2
6	Listing threats, vulnerabilities and controls in relation to all your classified information	0	0	0	0	0	1	1	1	2	2	2	3	3	3
	Listing impacts and risks in relation to all your classified information	0	0	0	0	0	0	0	1	2	2	2	2	2	3
7	Recording formal decisions and agreements about the risks you will manage	0	0	0	0	1	1	1	1	2	2	3	3	3	3
8	Generate list of risk management options	0	1	1	1	1	1	1	2	3	3	3	3	3	3

Process	**Process objectives**	**Level needed for each of the 14 segments in figure 2**													
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
9	Assignment of responsibility for carrying out your risk management activities	0	1	0	1	1	1	1	2	2	3	2	3	3	3
	Defining your prioritised risk management action plan and allocating resources	0	0	0	1	1	1	1	1	2	2	2	2	2	2
10	Defining and approving action plan reports and lists of activities to be undertaken	0	0	0	1	1	1	1	2	2	3	3	3	3	3
11	Coordinating risk management activities with other relevant projects (e.g. IT system updates, business continuity planning)	0	0	0	0	0	1	1	1	2	2	2	2	2	2
	Assigning and reporting on costs of risk management activities	0	0	1	1	1	1	1	1	1	2	2	2	2	2
12	Understanding residual risks (those left after controls have been implemented)	0	0	0	1	1	1	1	2	2	2	2	2	2	2
	Triggering iteration of threat and vulnerability assessment and decision activities	0	0	0	1	1	1	2	2	2	2	2	2	2	2
13	Deciding on how effectively risks have been managed and documenting this	0	0	0	1	1	1	1	2	2	2	2	3	3	3
14	Internal reporting on your management of risks and incidents	0	0	0	0	1	1	1	2	1	2	2	2	2	2
	External reporting on your management of risks and incidents	0	0	0	0	1	1	1	2	1	2	2	2	2	2
	Reporting on the cost effectiveness of your risk management	0	0	0	0	0	0	0	1	0	1	1	1	1	2
15	Delivering awareness of information risk management to all involved stakeholders (e.g. personnel and partners)	0	0	0	0	0	1	1	1	1	1	1	2	2	2
	Definition of a risk communication plan for the enterprise	0	0	0	0	0	1	1	1	1	1	1	1	1	2
	Referring to external risk management experts when appropriate	0	0	0	0	0	0	0	1	0	1	1	1	1	2

Table 1: Objectives for each of the 15 RA/RM processes for each of the 14 segments produced by the exposure and impact qualification questionnaire

6. Linking risk exposure and impact to existing RA/RM methodologies

WG3 has carried out detailed work to link the results of the risk exposure and impact questionnaire to the work carried out by WG2 on the characterization of existing RA/RM methodologies. In order to do this, each of the inputs and outputs to the 15 RA/RM processes (as identified by WG2) has been "weighted" in terms of its importance to the process and the weighted input and output requirements have been identified for each of the 14 segments shown in figure 2 above. Using these weighted inputs and outputs it is possible to plot the requirements for each process for all 14 segments and thus to match these against the input and output scores that were determined for a number of methodologies by WG2. This section describes the weighting process and shows the weighted input and output requirements for each of the 15 processes and 14 risk exposure and impact segments. This enables the segments to be compared with any RA/RM methodology that has been characterized using the same process; thus permitting the choice of methodologies that are most appropriate to the organization.

6.1. Weighting the process inputs and outputs

The requirement within each of the 14 segments of figure 2 for inputs and outputs connected with each of the 15 RA/RM processes has been weighted using possibility /necessity theory. This is a theory that deals with uncertain events in an alternative way to probability theory. It is particularly well-suited to modelling the likelihood of occurrence of factors, such as those under consideration here, with intentional (non-random) causes and where probability theory therefore does not apply [KLIR]. Possibility theory uses two scores to deal with the uncertainty of an event: the possibility of the event occurring (designated as "Pos" in table 2 below) and the impossibility of the event not occurring (designated as "Nec" in table 2 below). Each score is on a scale of between 0 and 1. Table 2 has been used by WG3 to weight the input and output requirements in each of the 15 RA/RM processes for each of the 14 exposure and impact types described above.

(Pos,Nec)	(Pos+Nec)/2	Description
(0.0, 0.0)	0.00	Neither useful nor needed
(0.5, 0.0)	0.25	Partly useful but not needed at all
(1.0, 0.0)	0.50	Fully useful, but not needed at all
(1.0, 0.5)	0.75	Fully useful and partly needed
(1.0, 1.0)	1.0	Fully useful and fully needed

Table 2: weighting table for RA/RM process inputs and outputs

6.2. Process inputs and outputs for exposure and impact segments

Table 3 shows the weighted input and output requirements for each of the 15 RA/RM processes for each of the 14 segments derived from the exposure and impact questionnaire (segments numbered as in section 4). This table also shows the "required process average" for each of the 15 processes in relation to each of the 14 segments. It will be noted that this average shows a basic requirement (1) where one or more of the inputs or outputs have such a requirement.

This table allows a more detailed analysis of an organization's RA/RM requirements to be carried out. It also permits an organization to match its RA/RM requirements with the most appropriate RA/RM methodology. This is examined in more detail in the next section.

Process	Input	Output	Segments resulting from exposure and impact questionnaire (see section 5)																											
			1		2		3		4		5		6		7		8		9		10		11		12		13		14	
			In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out
P.1 Definition of external environment	I.1.1	O.1.1	0	0	0	0	0	0	1	1	0	0	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2
	I.1.2	O.1.2	0	0	0	0	0	1	0	1	0	1	0	1	0	1	1	1	1	2	1	2	2	3	2	3	2	3	2	3
	I.1.3	O.1.3	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3	2	3	2
	I.1.4		0		0		0		0		0		0		0		1		1		1		1		2		2		2	
	I.1.5		0		0		0		1		0		1		1		1		1		2		2		2		2		2	
	Average		0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3
Required Process Average			0		0		0		1		0		1		1		1		1		2		2		2		2		2	
P.2 Definition of internal environment	I.2.1	O.2.1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3	2	3	2	3	3	3	3
	I.2.2	O.2.2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	3	2	3
	I.2.3	O.2.3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	3	2	3	3	3
		O.2.4		1		1		1		1		1		1		1		1		1		1		2		2		2		2
		O.2.5		0		0		0		0		0		0		1		1		1		1		2		2		2		2
		O.2.6		0		0		0		0		0		0		0		0		1		1		2		2		2		2
	Average		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2	3	3	3
Required Process Average			1		1		1		1		1		1		1		1		1		1		2		2		2		3	
P.3 Generation of risk management context	I.3.1	O.3.1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	2	2	2	2	2	3	2	3	3	3
	I.3.2	O.3.2	1	0	1	0	1	0	1	0	1	0	1	1	1	1	2	1	1	1	1	1	2	2	2	2	2	2	2	2
	I.3.3	O.3.3	1	0	1	0	1	0	1	0	1	0	1	1	1	1	2	1	2	1	2	2	2	2	2	2	2	2	2	2
	I.3.4	O.3.4	0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	2	1	1	2	2	2	2	2	2	2	2	2	2
	I.3.5		0		0		0		0		0		1		1		1		1		1		1		2		2		2	
	Average		1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	2	2
Required Process Average			1		1		1		1		1		1		1		2		1		2		2		2		2		2	
P.4 Formulation of impact limit criteria	I.4.1	O.4.1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	2	2	2	2	2	2	2	2
	I.4.2	O.4.2	0	0	0	0	1	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3	3	3	3	3
	Average		0	0	0	0	1	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3	3	3	3	3
Required Process Average			0		0		0		1		1		1		1		2		2		2		2		3		3		3	
P.5 Identification of risks	I.5.1	O.5.1	0	1	0	1	0	1	0	1	1	1	1	1	1	1	2	1	1	1	2	2	2	3	3	3	3	3	3	3
	I.5.2	O.5.2	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	1	1	2	1	2	2	2	2	2	2	3	3
	I.5.3	O.5.3	0	1	0	1	0	1	0	1	0	2	0	2	0	3	0	3	0	1	1	1	1	2	1	2	1	3	1	3

Process	Input	Output	Segments resulting from exposure and impact questionnaire (see section 5)																											
			1		2		3		4		5		6		7		8		9		10		11		12		13		14	
			In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out
	I.5.4	O.5.4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	1	1	1	2	1	2	1	2	1	2
		O.5.5		0		0		0		1		0		1		1		1		2		2		2		2		2		2
		O.5.6		0		0		0		0		0		0		0		0		1		1		1		1		1		1
		O.5.7.		0		0		0		0		0		1		1		1		1		1		2		2		2		2
	Average		0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
Required Process Average			0		0		0		0		0		1		1		1		1		1		2		2		2		2	
P.6 Analysis of relevant risks	I.6.1	O.6.1	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	2	2	2	2	3	2	3	2	3	3	3	3
	I.6.2	O.6.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	2	2	1	2	2	3	2	3	3	3
	I.6.3	O.6.3	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	2	2	2	2	2	2	2	2	3	3	3	3	3
	I.6.4	O.6.4	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	2	2	2	2	2	2	3	2	3	2	3	2
		O.6.5		0		0		0		0		0		0		0		1		2		2		2		2		2		2
		O.6.6		0		0		0		0		0		0		0		1		1		1		2		2		2		2
	Average		0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	2	2	2	2	2	2	3	2	3	3	3	3
Required Process Average			0		0		0		0		0		0		1		1		2		2		2		2		3		3	
P.7 Evaluation of risks	I.7.1	O.7.1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3
	I.7.2		0		0		0		0		0		0		0		1		1		2		2		2		2		3	
	Average		0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3
Required Process Average			0		0		0		0		1		1		1		1		2		2		3		3		3		3	
P.8 Identification of options	I.8.1	O.8.1	0	0	0	1	0	1	0	1	1	1	1	1	1	1	1	2	2	2	2	3	2	3	2	3	2	3	2	3
	I.8.2		1		1		1		1		1		1		1		1		2		3		3		3		3		3	
	I.8.3		0		0		1		1		1		1		1		1		2		2		2		2		2		2	
	Average		0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3	2	3	2	3	2	3	2	3
Required Process Average			0		1		1		1		1		1		1		1		2		2		2		2		2		2	
P.9 Development of action plan	I.9.1	O.9.1	0	0	1	1	0	1	1	1	1	1	1	2	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3
	I.9.2	O.9.2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2	2
	I.9.3	O.9.3	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	2	1	2	1	3	1	2	1	3	1	3	1	3
	I.9.4		0		0		0		1		1		1		1		1		1		1		1		1		1		1	
	Average		0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	2	1	2	2	3	2	2	2	3	2	3	2	3
Required Process Average			0		0		0		1		1		1		1		2		2		2		2		2		2		2	
P.10 Approval of action plan	I.10.1	O.10.1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	3	2	3	2	3	2	3	2	3	2
	I.10.2		0		0		0		1		1		1		1		1		1		1		1		1		1		1	
	Average		0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2
Required Process Average			0		0		0		1		1		1		1		2		2		2		2		2		2		2	

Process	Input	Output	Segments resulting from exposure and impact questionnaire (see section 5)																											
			1		2		3		4		5		6		7		8		9		10		11		12		13		14	
			In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out
P.11 Implementation of action plan	I.11.1	O.11.1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	2	1	2	1	2	1	2	1	2	1	2	1
	I.11.2	O.11.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	1	2	2	2	2	2	2	2	2	2	2
	I.11.3	O.11.3	0	0	0	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	I.11.4	O.11.4	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	2	1	2	1	2	1	2	1	2	1	2	2
	Average		0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	2	1	2	1	2	1	2	1	2	1	2	2
Required Process Average			0		0		0		1		1		1		1		1		1		2		2		2		2		2	
P.12 Identification of residual risks	I.12.1	O.12.1	0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
		O.12.2		0		0		0		1		1		1		1		2		2		3		2		3		3		3
	Average		0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	2	2	2	3	2	3	2	3
Required Process Average			0		0		0		1		1		1		1		2		2		3		2		3		3		3	
P.13 Risk acceptance	I.13.1	O.13.1	0	0	0	0	0	0	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2	3	3	3	3	3	3
	I.13.2		0		0		0		1		1		1		1		2		2		2		2		2		2		2	
	Average		0	0	0	0	0	0	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2	3	3	3	3	3	3
Required Process Average			0		0		0		1		1		1		1		2		2		2		2		3		3		3	
P.14 Risk indicator gathering and reporting	I.14.1	O.14.1	0	0	0	1	0	1	0	1	1	1	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	2	3
	I.14.2	O.14.2	0	0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	3	2
	I.14.3	O.14.3	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2
	I.14.4	O.14.4.	0	0	1	0	1	0	1	0	1	0	2	0	2	0	2	1	1	0	2	1	2	1	3	1	3	1	3	2
	I.14.5		0		0		0		1		1		1		1		1		1		2		2		2		2		2	
	I.14.6		0		0		0		0		0		0		0		1		0		1		1		1		1		2	
	Average		0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	2	1	1	2	2	2	2	2	2	2	2	2	2
Required Process Average			0		0		0		0		1		1		1		1		1		2		2		2		2		2	
P.15 Risk communication, awareness and consulting	I.15.1	O.15.1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	2	2
	I.15.2	O.15.2	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
	I.15.3	O.15.3	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2
	I.15.4	O.15.4.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	1	1	1	1	2	2
	I.15.5		0		0		0		0		0		0		0		1		0		1		1		1		1		2	
	Average		0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
Required Process Average			0		0		0		0		0		1		1		1		1		1		1		2		2		2	

Table 3: Weighted input and output requirements for each of the 15 RA/RM processes for each of the 14 segments derived from the risk exposure and risk impact questionnaire (segments numbered as in section 5)

7. Uses of the results from this approach

This approach has been used, on a trial basis, with a number of organizations that took part in an ENISA-sponsored conference in 2007. The use, with these organizations, of the questionnaire shown in section 3 of this paper enabled WG3 to be sure that the approach it has taken was both viable and capable of producing results that may be of value to organizations. The potential value of this approach is explored in this section.

7.1. Developing awareness and understanding

Many organizations, especially those that are small- or medium-sized, do not have the resources needed to devote sufficient effort to developing awareness and understanding of their information risk and how it can best be managed. The use of the questionnaire shown in section 3 of this paper enables such organizations to appreciate, in a simple and easily comprehended format, the most significant factors that they need to consider in this area. By drawing attention to the causes of threats and vulnerabilities, and the potential impact that these could have on the business, the questionnaire highlights the factors to which the organization needs to devote attention. It does this in non-technical, business-oriented language in order to help ensure that all parts of the organization develop an appropriate level of awareness and understanding of the issues at stake as a result of information risk.

7.2. Triggering decisions

The 14 groups described in section 5 of this paper are intended to assist organizations to make appropriate decisions regarding their actions in relation to the assessment and management of information risk. Categorization into one of the 14 segments, as a result of completing the questionnaire in section 3, will be particularly helpful to small- or medium-sized organizations with few resources devoted to information security. Using the lists of requirements and recommendations in section 5, such organizations will be triggered to make appropriate decisions about the next steps they need to take to monitor and manage their information risk.

7.3. “What if” scenario planning

The ability to plan ahead is also potentially delivered by use of the questionnaire in section 3, and the description of the 14 resulting segments of exposure and impact in section 5. If an organization is, for example, planning to expand its online business, it can answer the questions posed in section 3 as if it was already in that position. An online business will be more exposed to threats, will have more use of the Internet, may have more regulatory exposure and will be more impacted by loss of its IT systems. By comparing its current requirements for information risk assessment and treatment, with those that it might require following an expansion of its online business, an organization will be able to appreciate those areas in which it will need to improve and expand its information risk management capabilities. Such data could be of assistance in making an informed business decision.

7.4. Choosing an appropriate RA/RM methodology

In order to choose an appropriate methodology it is necessary for an organization to determine its risk exposure and impact segment and then to compare the required processes and their inputs and outputs for that segment with the corresponding processes, inputs and outputs for a methodology that has been characterised.

Figure 3, below, shows the required process averages for the hypothetical example organization (as illustrated in figures 1 and 2). Figure 4 shows the process averages for the IT Grundschutz RA/RM methodology and figure 5 shows the same for the NIST SP 800-30 RA/RM methodology.

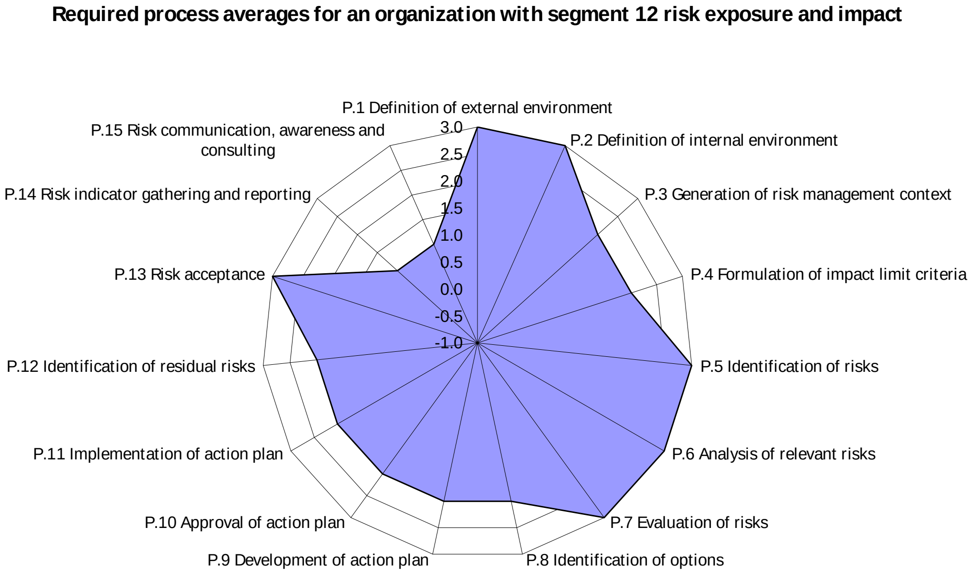


Figure 3: Required RA/RM process averages for ENISA derived from the risk exposure and risk impact questionnnaire

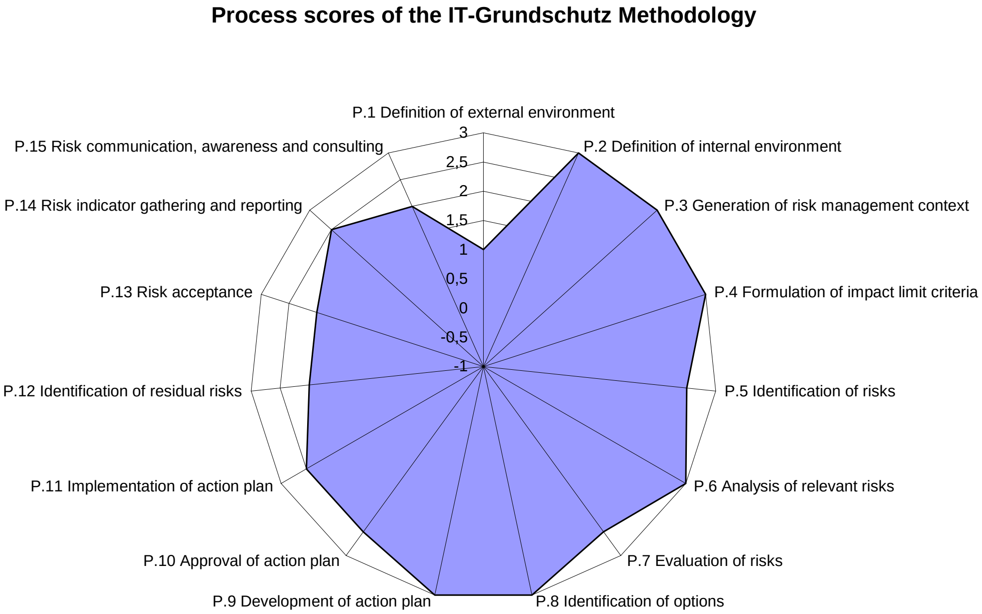


Figure 4: Process scores for the IT-Grundschutz RA/RM methodology

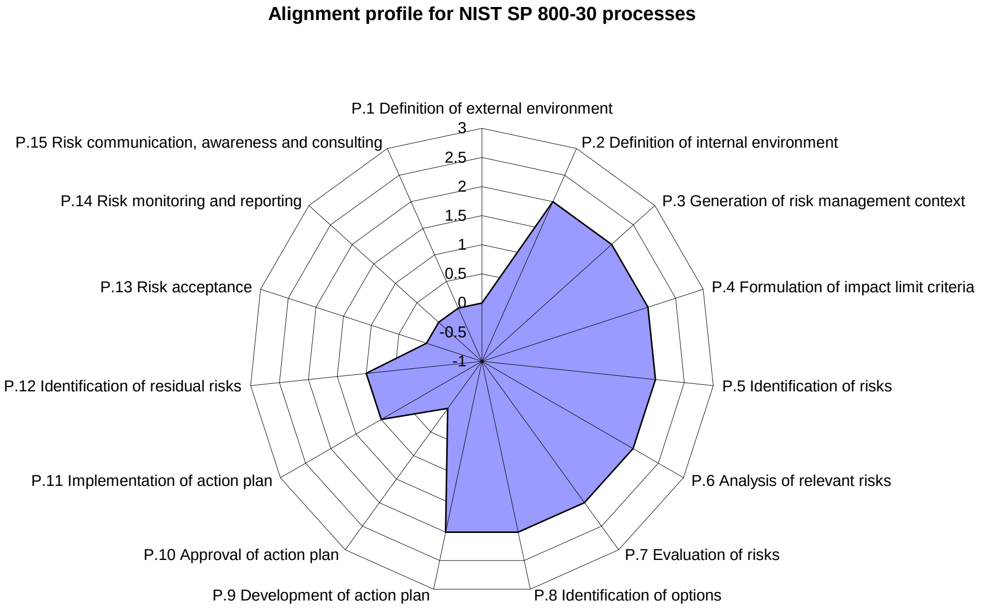


Figure 4: Process scores for NIST SP 800-30 RA/RM methodology

From a comparison of the diagrams above it will be seen that overall the IT-Grundschutz methodology is probably more appropriate for use in the example organization shown in figure 1 (ENISA) than the NIST methodology. However, there are areas where the IT-Grundschutz methodology are probably un-necessarily complex and where the NIST methodology may be more appropriate: such as the generation of the risk management context and the formulation of the risk impact criteria. And there are some processes, such as the definition of the external environment and risk acceptance, where neither methodology is adequate.

Table 3 will also enable a more detailed comparison to be made between the input and output requirements for individual processes for an organization, and the inputs and outputs to and from the same process within a characterised methodology. Figure 5 below, shows the comparison between the requirements for the example organization (ENISA) (as determined by the risk exposure and risk impact questionnaire) and the IT-Grundschutz methodology for the outputs from the identification of risks process (P.5).

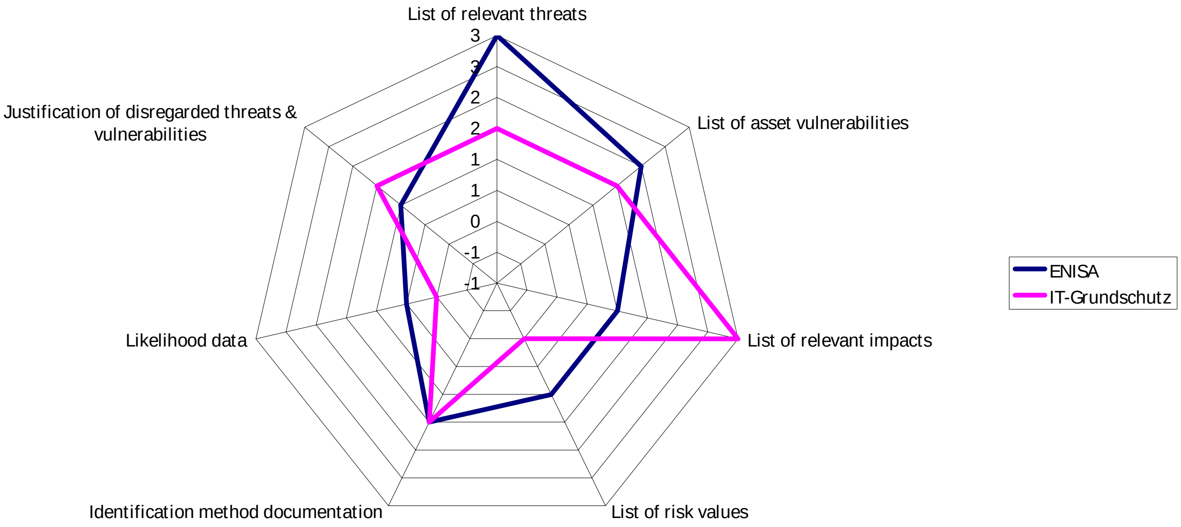


Figure 5: Comparison of outputs generated by IT-Grundschutz P.5 and hypothetical example requirements

It will be seen from figure 5 that the IT-Grundschutz methodology used to generate risk identification outputs is only appropriate to the example organization (ENISA) in its identification of method documentation. In other outputs for this process, IT-Grundschutz is likely to be either inadequate or overly complex.

8. Further work

The ENISA RA/RM WG3 has identified a number of areas in whch the work described in this paper might be carried forward. Amongst these are the following:

- Developing the ability to compare RA/RM methodologies, as outlined in section 7.4 of this paper.
- Analysis of further methodologies, including more granular analysis of the use of input/output data.
- The development of comparative radar diagrams for methodologies, their inputs and outputs.
- Web-based publication of tools based on the work described in this paper.
- Collection of additional data about the use of the methodology described in this paper, especially with small- and medium-sized businesses.
- Production of a report based on data collected about the use of the methodology by small- and medium-sized businesses.
- Translation of this paper and the questionnaire into other European languages.
- Development of cases studies showing how the tools described here can be used in practice.
- Development of this work in combination with other work being done by ENISA with small- and medium-sized businesses.
- Development of tools to enable organizations to assess their current effectiveness assessment – leading to gap analysis that will point the way to a prioritised action plan.
- Analysis of the relationship between information risk and legal and regulatory requirements, benchmarked for different business sectors.

9. Conclusion

In conclusion, this document aims to provide all that is needed by an organization to profile its exposure and potential impact at a high level and to understand its RA/RM requirements that relate to this profile. The exposure and risk impact questionnaire outlined in section 3 of this document can be analyzed as described in section 4 to produce a description of the risk assessment and management measures that an organization needs to consider, as described in section 5. It is also able to generate more detailed recommendations for risk assessment and management requirements, as shown in table 1.

In addition, as explained in section 6, the risk exposure and risk impact analysis is also able to generate a process, shown in table 3, that enables an organization to consider which existing RA/RM methodologies are best suited to meet its requirements. These can be considered graphically at either the RA/RM process level, or at the more detailed level of inputs to and outputs from those processes, as shown in 7.4.

Finally, ENISA will produce a tool (the Self Assessed Risk Profiler (SARP)) that is able to generate the risk profile for an organization and automatically deliver the appropriate description of its risk assessment and management objectives and relevant charts.

10. References

[KLIR] KLIR, George.,J.; WIERMAN, Mark.,J.; Uncertainty-based-Information. Elements of Generalized Information Theory. PHYSICA-VERLAG, 1999 (See chapter 2)

[EBIOS] Maturité SSI. Approche méthodologique. Version 2007-11-02. Available at: http://www.ssi.gouv.fr/fr/confiance/documents/methodes/maturitessi-methode-2007-11-02.pdf