ENISA ad hoc working group on risk assessment and risk management

Methodology for evaluating usage and comparison of risk assessment and risk management items

Deliverable 2
Version 1

Date: 26/04/2007

Index of Contents

1 Concept and Purpose

The ENISA ad-hoc working group on risk assessment and management (referred to in this document as "the Working Group") has determined a methodology to allow direct comparison between items that enable organizations to perform risk assessment and risk management. The methodology considers the processes of risk assessment and management items, together with the inputs and outputs to these, and scores these against a benchmark set of processes, inputs and outputs, as determined by the Working Group.

The purpose of the methodology is to allow one or both of the following to be performed:

- Determination of the most appropriate risk assessment and management items for use by organizations in a range of given circumstances; such as their business sector, size, culture, legal, regulatory and governance requirements, as well as the sophistication of their risk management approach and the resources available to them.
- Direct comparison between two or more risk assessment or management items in order to permit expert advice to be given on their suitability for use in particular circumstances.

2 Terms

The following terms are used in this document.

Term	**Definition**
Benchmark	A set of possible risk assessment and management processes (qv), inputs (qv) and outputs (qv) defined by the ENISA ad-hoc working group on risk assessment and management and used as a reference in this paper.
Characterisation	Methodology for defining any item (qv) in relation to the Benchmark (qv)
Alignment	Scoring the processes (qv), inputs (qv) and outputs (qv) of an item (qv) in relation to the Benchmark (qv)
Alignment profile	Radar chart showing the results of scoring the processes (qv), inputs (qv) and outputs (qv) of an item in relation to the Benchmark (qv)
Input	Information and data required by a process (qv) in order to allow it to function as intended
Item	A tool, code of (good) practice or methodology in use for risk assessment or risk management or both.
Output	Result produced by a process (qv) that enables an item (qv) to deliver useful functionality.
Process	Operation performed on input (qv) by an item (qv) in order to produce an appropriate output (qv)

Term	Definition
Use case	A set of defined circumstances under which an item (qv) might be used; determined by the user's business sector, size, culture, legal, regulatory and governance requirements, sophistication of its risk management approach, available resources and other factors.

3 Benchmark processes, inputs and outputs

The Working Group has defined a benchmark set of the possible processes, inputs and outputs that organizations might expect to see incorporated into items used in the assessment and management of information risk; these are referred to in the rest of this paper as "the Benchmark". The Benchmark has been compiled from the range of items studied by the Working Group, and is based on both the experience of Working Group members and on the process described on the ENISA website (www.enisa.europa.eu/rmra/rm_process.html). The Benchmark is shown in Annex A of this document. The Benchmark divides risk assessment and management into the following five stages and 15 processes:

- Stage A: Definition of scope and framework:
  - 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
- Stage B: Risk assessment:
  - P.5 Identification of risks
  - P.6 Analysis of relevant risks
  - P.7 Evaluation of risks
- Stage C: Risk treatment:
  - 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
- Stage D: Risk acceptance
  - P.13 Risk acceptance
- Stage E: Risk monitoring and review
  - P.14 Risk monitoring and reporting
- Stage F: Risk communication, awareness and consulting
  - P.15 Risk communication, awareness and consulting

It is possible to "characterise" an item in relation to the Benchmark by comparing an item's processes, inputs and outputs with their equivalents as described in the Benchmark at Annex A. This is done using the methodology explained in section 4 below. Characterisation of items enables an organization to perform one or more of the following functions:

1. Determine the suitability of a characterised item as it relates the overall requirements of the organization, by referring to the "use cases" discussed in section 5.
2. Characterise a particular item to determine if is suitable for use in specific circumstances, as discussed in section 6.
3. Objectively compare two or more characterised items in order to see their relative strengths and weaknesses, as discussed in section 7.

4 Characterisation methodology

Characterisation of an item is undertaken by comparing a description of the item with the descriptions given in the Benchmark at Annex A. An item is characterised by evaluating it in relation to the Benchmark. The evaluation is made by assigning a score to the item's processes, and to the inputs and outputs of those processes, according to the degree of convergence these have to their equivalents in the Benchmark. The scores for processes should be determined using table 1.

Score	Convergence of item process with equivalent Benchmark process
0	Process not mentioned at all
1	Process described as part of the item with an external process referenced
2	Process described in some detail with simple instructions
3	Process very highly detailed and exhaustive

Table 1: Scoring for processes

If an item's processes are considered to occupy a position that is intermediate between the descriptions above, an intermediate score (such as 1.5) may be given.

The scores for inputs and outputs to and from processes should be determined using table 2.

Score	Convergence of item's input/output with equivalent Benchmark input/output
0	Input/output not mentioned at all
1	Input/output described with reference to an external process
2	Input/output described in some detail with simple instructions
3	Input/output described in great detail with exhaustive instructions

Table 2: Scoring for inputs to, and outputs from processes

Again, if the inputs or outputs are considered to occupy a position that is intermediate between the descriptions above, an intermediate score (such as 1.5) may be given.

It will be seen that an item can be characterised on the basis of an evaluation of its processes, or of its inputs or its outputs. For broad comparison purposes, characterisation on the basis of

processes will be sufficient. This will enable an “alignment profile” to be drawn on the basis of the scores for each of the 15 processes.

On the other hand, characterising an item on the basis of an evaluation of the inputs to, or outputs from, its processes, will give a more granular result. In this case an alignment profile should be produced for individual processes.

Once an item has been evaluated according to the scoring systems described above, an alignment profile can be produced, by plotting the scores for each process on a radar chart. Examples of such alignment profiles for processes in the IT-Grundschutz methodology from the German BSI are given in figures 1 to 3. Please note that these figures are derived from Annex B, which shows the entire IT-Grundschutz methodology compared with the Benchmark.

An alignment profile for the processes of the entire IT-Grundschutz methodology is given in figure 1.

Figure 2 shows the alignment profile for inputs to process P.5 (identification of risks) for IT-Grundschutz and figure 3 for the IT-Grundschutz outputs from the same process. It will be recognised that the two alignment profiles are different, indicating that the process has some variations in its requirements for input and in the degree of output that it produces. This variability could be of significance when selecting an item for a particular use (see sections 6 and 7 below).

It will be noted that the axes of the chart have been scaled to start at -1, this is to avoid the problem of ‘blank’ cells should a process have a zero score.

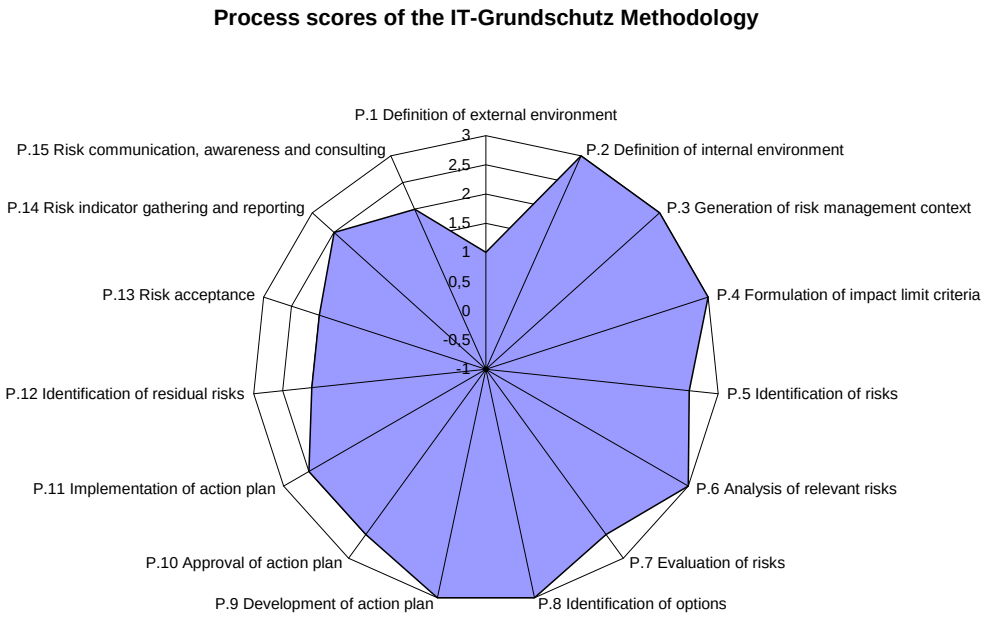

Figure 1: Alignment profile generated by IT-Grundschutz processes

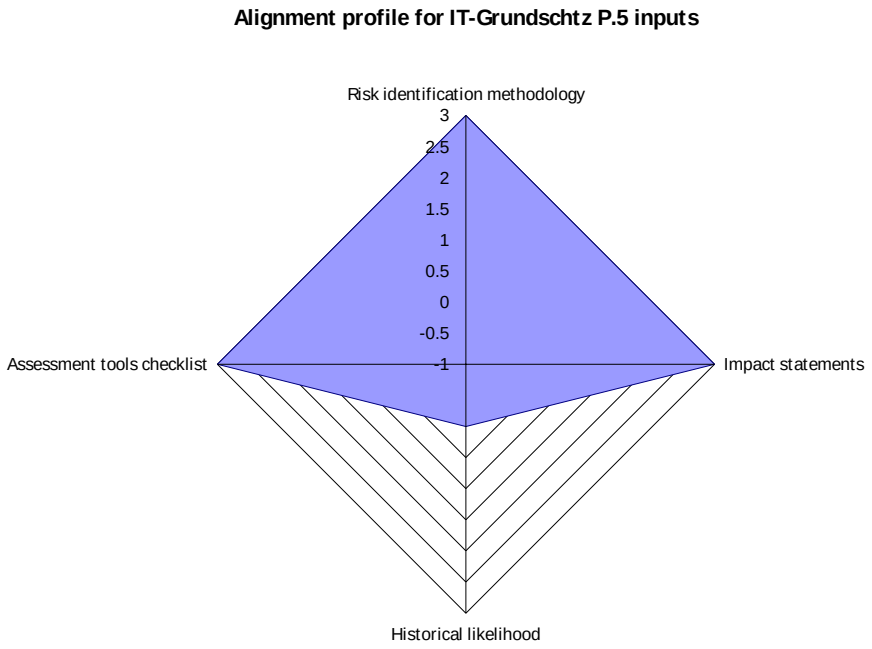

Figure 2: Alignment profile generated by IT-Grundschutz inputs to process P.5

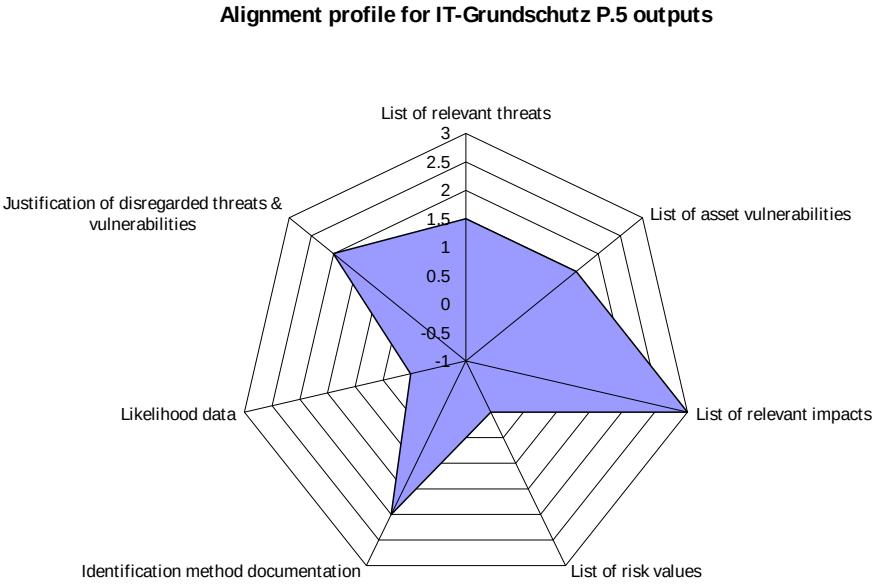

Figure 3: Alignment profile generated by IT-Grundschutz outputs from process P.5

5 Determining overall organizational requirements

Organizations may wish to determine their overall requirement for a risk assessment and management methodology by considering a number of "use cases". An organization wishing to do this should look at the examples given in table 3 below. The Working Group has identified five use cases. These are listed in table 3, together with examples of the type of organization that might be typical of each use case and a brief description of the risk assessment and management (RA/RM) requirements that might be appropriate to each type of organization.

Nr	Type	Example	RA/RM Requirements
1	Small business, where Internet usage is not part of the business processes. No dedicated IT-resources.	Small shop, small professional consultancy businesses (including law, architecture etc.)	Understand critical business assets, threats and vulnerabilities. Plan and implement appropriate countermeasures
2	Small to medium-sized business with more extensive Internet usage, where Internet is core to the business process	Small e-commerce businesses, small media businesses	Understand critical business assets, threats and vulnerabilities and conduct a risk analysis. Plan and implement appropriate countermeasures. Identification of residual risks. Risk monitoring and reporting
3	Medium-sized private business with simple governance requirements	Private trucking, logistic, manufacturing and publishing companies.	Understand critical business assets, threats and vulnerabilities and conduct a risk analysis. Develop and implement action plan. Define procedures for risk acceptance, monitoring and internal communication of these.
4	Medium to large-sized business with more complex governance requirements	Food companies, insurance, companies, all those types of organization in 3 that are also public companies.	Define the scope of their internal and external requirements. Apply well-defined processes and procedures for risk assessment, risk management and monitoring and internal and external communication of these.

Nr	Type	Example	RA/RM Requirements
5	Large-sized business with rigorous governance requirements	Pharmaceutical, chemical, energy, telecommunications, utilities and banking.	Define the scope of their internal and external requirements. Apply well-defined and clearly communicated processes and procedures for risk assessment and risk management as well as detailed monitoring, auditing and communication processes for both internal and external use.

Table 3: Use cases for risk assessment and risk management

The Working Group has evaluated scores for the processes that would be appropriate to each of the five use cases described above. These scores have been used to produce a series of alignment profiles for processes that are illustrated in the radar diagrams in sections 5.1 to 5.5 below.

These alignment profiles are illustrative only. It is intended that users compare the alignment profile that is most appropriate to their circumstances to those of a range of items (for example see section 7). This will enable them to make a preliminary selection of the item, or items, that might be most appropriate to their circumstances. However, organizations are expected to refine this process by producing their own individual alignment profile. Using this, a more accurate selection of items can be made.

5.1 Small business with limited Internet usage

Figure 4 shows a process alignment profile for this use case. The requirements of a small business are based on the following assumptions:

- The external IT risk is low, because the Internet is not core to the business, and can be simply managed using “off-the-shelf” technology and the internal environment is simple due to the small size of the business. The risk management context and impact limit criteria are therefore obvious to the management, and do not require extensive analysis.
- Identification and analysis of risks, however, may be more complex as a result of limited understanding of the IT systems in use.
- Evaluation of risks, identification of options, definition of action plan and approval are easily and simply achieved by the small number of individuals involved. Although implementation of an action plan requires that some procedures need to be defined and implemented.
- Identification of residual risks and risk acceptance can be carried out easily and simply by the small number of individuals involved.
- Risk communication, awareness and consulting can be implemented intuitively, well defined processes are not therefore required.

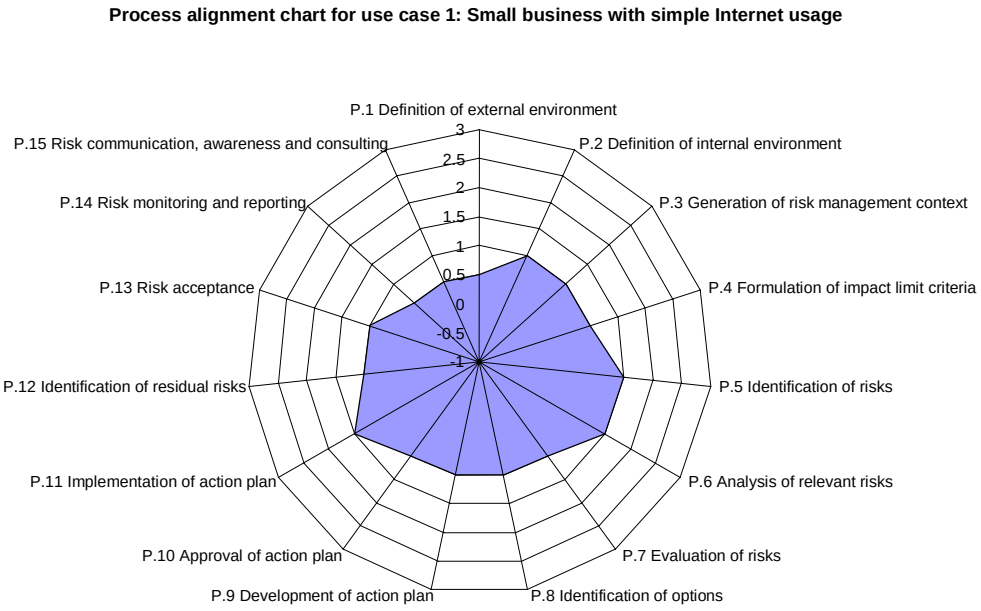

Figure 4: Alignment profile for use case 1: Small business with simple Internet usage

5.2 Small to medium-sized business with more extensive Internet usage

Figure 5 shows a process alignment profile for this use case. The requirements of a small to medium-sized enterprise, in which the Internet is business-critical, are based on the following assumptions:

- The external IT risk is higher, because the Internet is business-critical and the internal IT risk is higher, because IT systems are business-critical. The risk management context must therefore be more carefully analysed and the impact limit criteria must be more precisely determined in relation to the business.
- Identification and analysis of risks will also be more complex because of the business's dependency on IT systems, which may be more complex than can be easily managed.
- Evaluation of risks and identification of options are not evident and need defined, reliable processes and procedures.
- Because of its complexity, the action plan should be developed by specialists, with formal approval by management.
- Implementation of action plan requires the use of defined, reliable processes and procedures.
- Identification of residual risks must be carried out carefully, to safeguard business-critical systems.
- Risk acceptance processes and procedures are simple because of the small size of the organization.
- Risk monitoring and reporting must be reliable, but need not be complex because of the small size of the organization.

- Communication, awareness and consulting will also be relatively simple because of the small size of the organization.

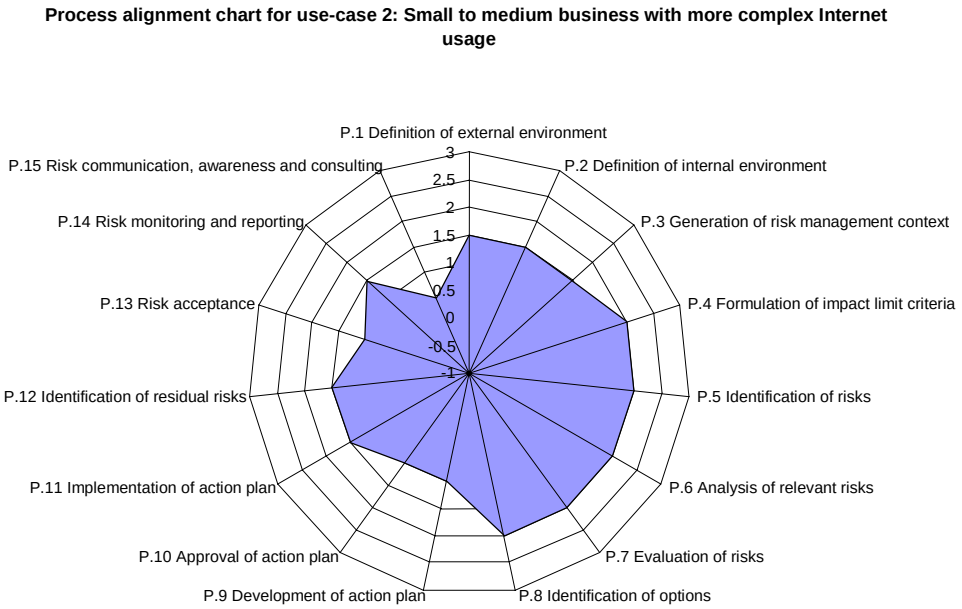

Figure 5: Alignment profile for use case 2: Small to medium-sized business with more complex Internet usage

5.3 Medium-sized private business with simple governance requirements

Figure 6 shows a process alignment profile for this use case. The requirements of a medium-sized private business with simple governance requirements are based on the following assumptions:

- The external and internal IT risk is somewhat higher as a result of the business size and complexity. This accordingly demands more complex analysis of the risk management context and defined processes and procedures to determine the impact limit criteria and provide comparability.
- The size and complexity of the business will also require more complex identification, analysis and evaluation of risks, together with clearly defined, reliable processes and procedures.
- The size and greater complexity of the organization may also require specialist input into the development of the action plan, as well as clearly defined approval procedures for it.
- Implementation of action plan will require a clearly defined roll-out and associated control procedures
- The size and greater complexity of the organization also require more careful identification of residual risks and a clearly defined process for risk acceptance.
- As a result of the size and greater complexity of the organization, risk monitoring and reporting processes and procedures will be needed, as will improved risk communication, awareness and consulting.

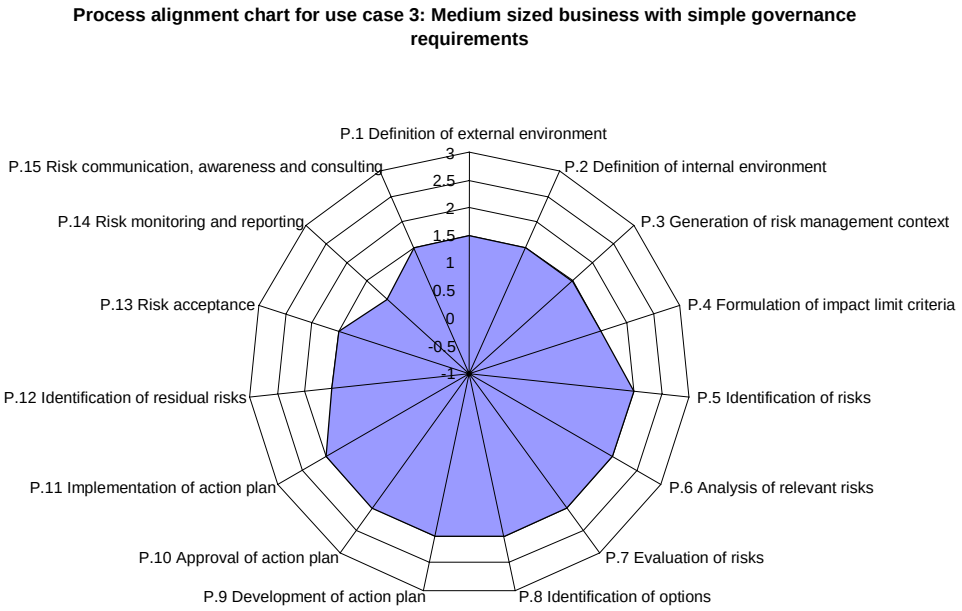

Figure 6: Alignment profile for use case 3: Medium-sized business with simple governance requirements

5.4 Medium to large-sized business with more complex governance requirements

Figure 7 shows a process alignment profile for this use case. The requirements of a medium-to-large-sized, publicly-quoted company are based on the following assumptions:

- External and internal IT risks are highly complex, requiring precise analysis of the risk management context and well-defined impact limit criteria.
- Identification and analysis of risks are complex and have to be carried out carefully.
- Evaluation of risks and identification of options are also complex, requiring well defined processes and procedures.
- The action plan must be developed by specialists and will require well-defined and clearly set-out approval procedures, which must be auditable.
- Implementation of action plan requires the definition of clearly defined roll-out and control procedures.
- The identification of residual risks must be subject to well defined, auditable procedures and decisions on risk acceptance must follow traceable, reproducible and auditable processes and procedures.
- Processes and procedures for risk monitoring and reporting must be well defined and auditable.
- Processes for risk communication, awareness and consulting must be clear, well implemented and auditable.

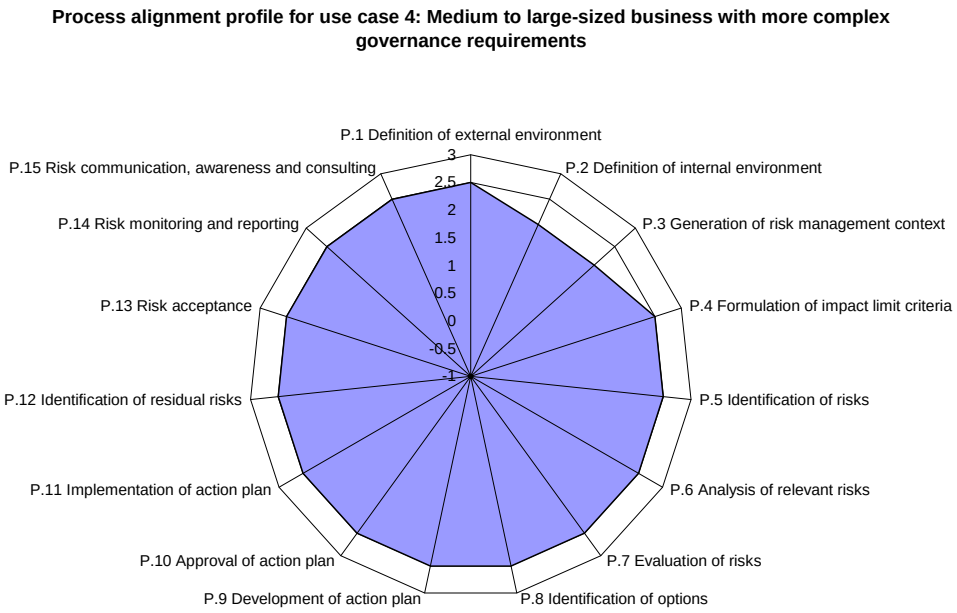

Figure 7: Alignment profile for use case 4: Medium to large-sized business with more complex governance requirements

5.5 Large-sized business with rigorous governance requirements

Figure 8 shows a process alignment profile for this use case. The requirements of a large-sized business with rigorous governance requirements are based on the assumption that the size, complexity and audit requirements of such organizations will require that the utmost attention should be paid to all aspects of risk assessment and management. It is therefore assumed that such an organization will have detailed and complex requirements for processes in all three stages.

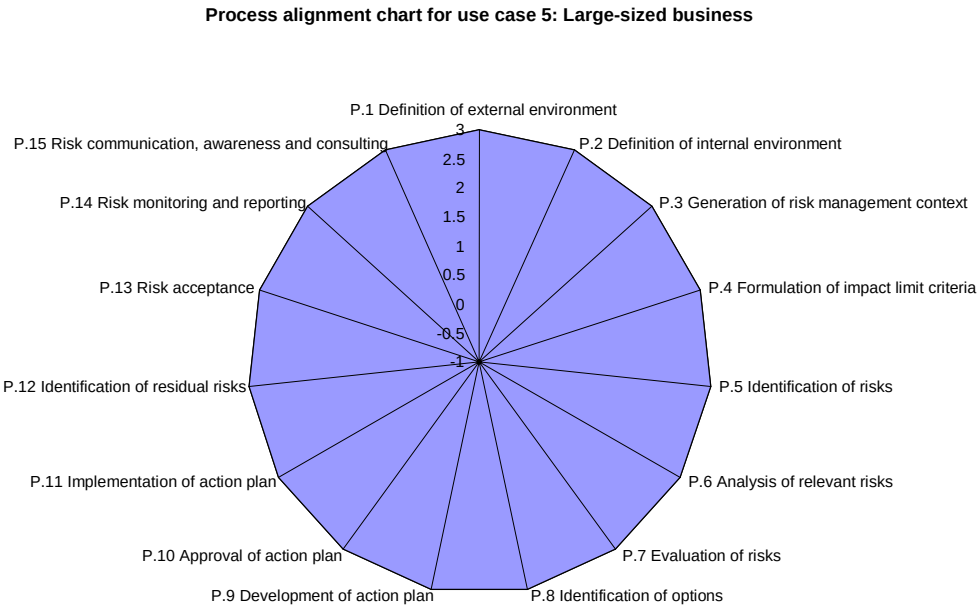

Figure 8: Alignment profile for use case 5: Large-sized business

6 Identification of an item for specific use

An alignment profile can be drawn for any item. This can then be used to determine if an item is most suitable for a use case relevant to a particular organization. Or to an organization's own required alignment profile, which might (for example) be determined by its individual ability to provide inputs and/or outputs to an RA/RM methodology.

As examples: figure 9 shows the alignment profile for the processes of NIST SP 800-30; figure 10 shows the alignment profile for the processes of Dutch A&K Analysis and; figure 11 shows the alignment profile for the processes of ISO/IEC 17799:2005. Annex B contains tables showing the full comparison between the NIST, Dutch A&K and ISO 17799 methodologies and the Benchmark. A description of these items, and IT-Grundschutz (whose alignment profiles are shown in figures 1 to 3), can be found at the ENISA website under: http://www.enisa.europa.eu/rmra/rm_ra_methods.html.

Organizations may also wish to select particular processes from different items in order to perform specific functions. For example, although a smaller organization may feel it appropriate to use the NIST methodology overall, it may decide that its circumstances require a more detailed analysis of its risk identification (P.5). In which case it would look at the alignment profiles for the inputs and outputs to that particular process for a number of other items. An example of a comparison of inputs and outputs to a particular process is discussed in the next section (see figures 12 and 13).

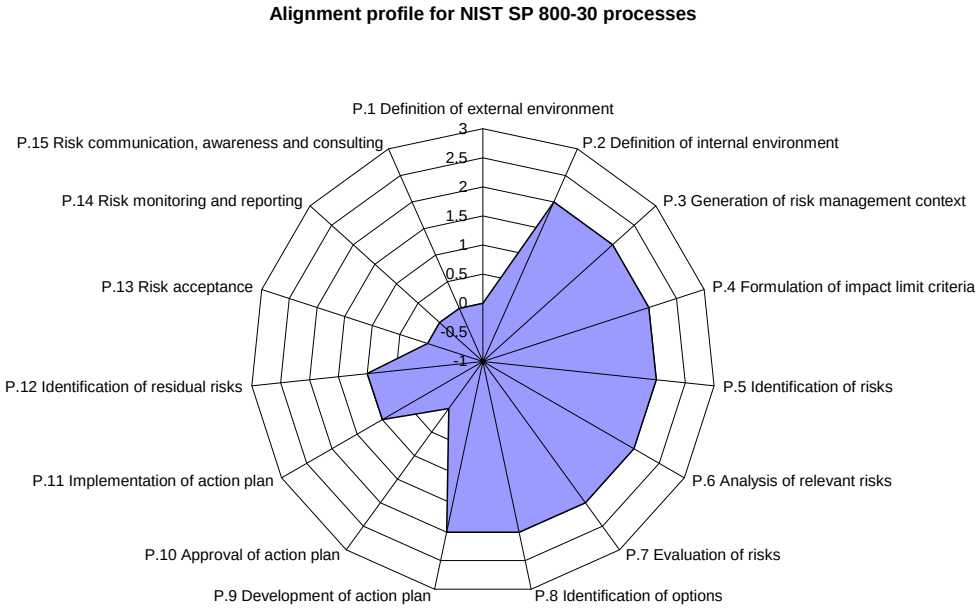

Figure 9: Alignment profile of NIST SP 800-30 processes

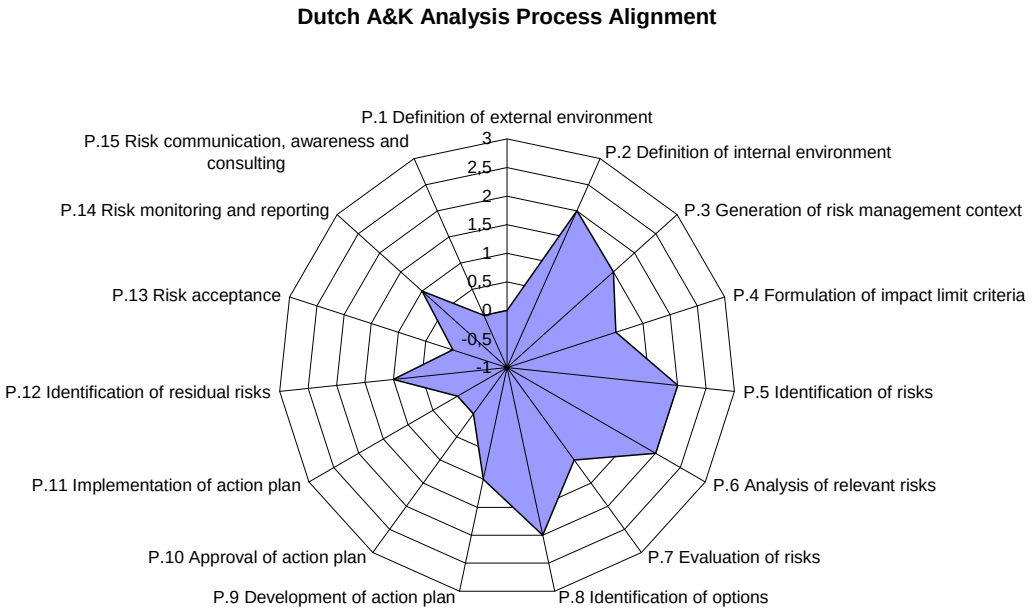

Figure 10: Alignment profile of Dutch A&K Analysis processes

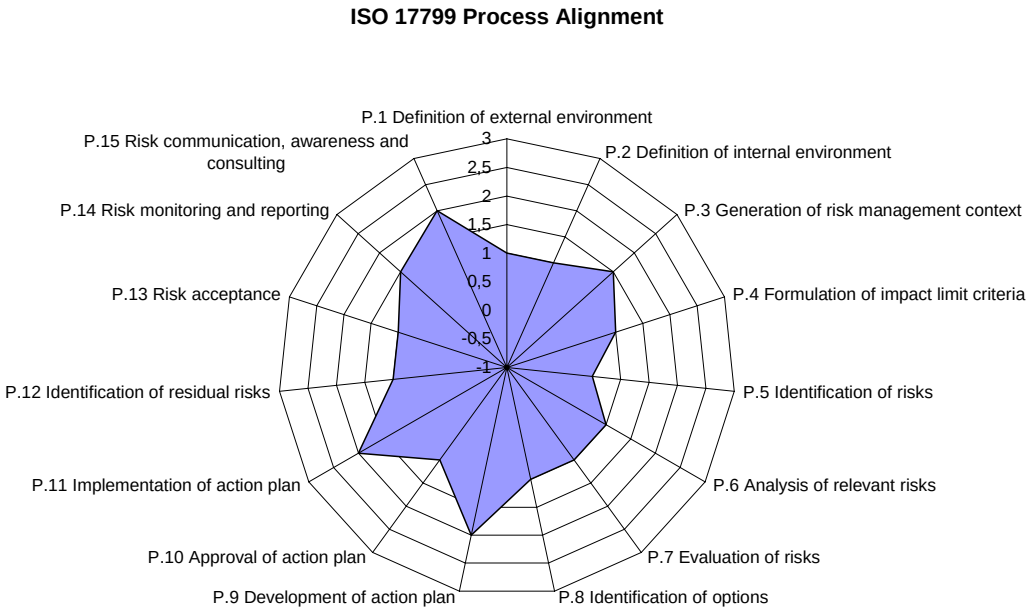

Figure 11: Alignment profile of ISO/IEC 17799:2005 processes

7 Direct Comparison between items

Alignment profiles for two or more items can also be used to compare the relative coverage of those items. At figure 12 is a comparison between the alignment profiles of IT-Grundschutz processes and NIST SP 800-30 processes.

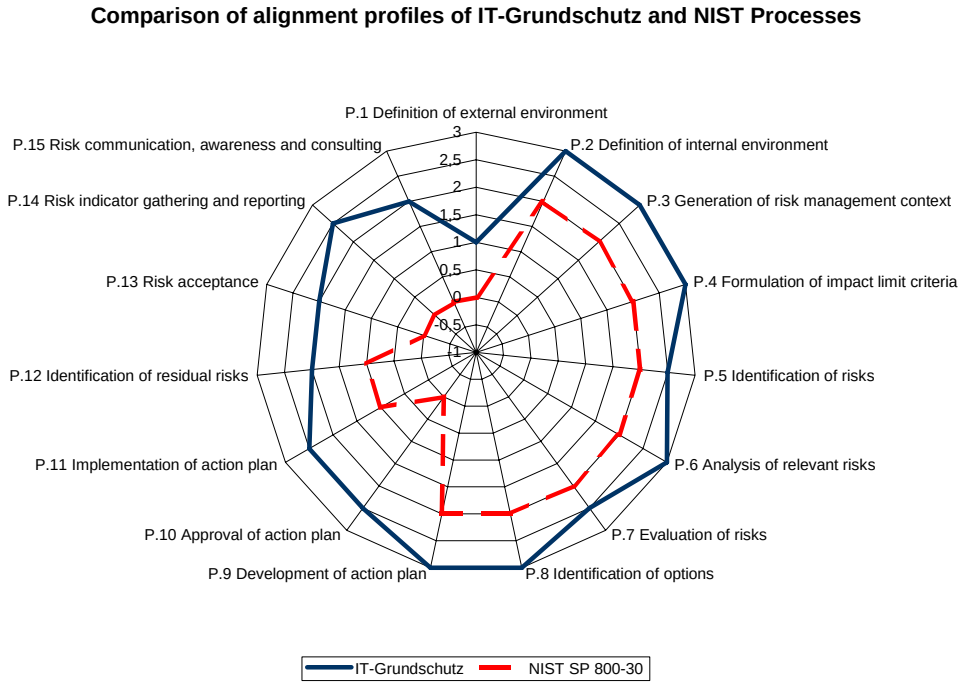

Figure 12: Comparison of alignment profiles of IT-Grundschutz and NIST processes

Figure 12 clearly shows that the coverage of the IT-Grundschutz methodology is far broader and deeper than that of NIST, and should therefore be considered for use by large organizations, as comparison with figures 7 and 8 would indicate. However, it also shows that the NIST methodology would probably be better suited to deployment by small- or medium-sized businesses, as comparison with figures 4 and 5 will indicate.

More granular comparison between items can take place at the level of inputs to, and outputs from, processes. Figure 13 compares the inputs to P.5 for IT-Grundschutz and NIST and Figure 14 shows the comparison for the outputs of P.5 for the same two methodologies.

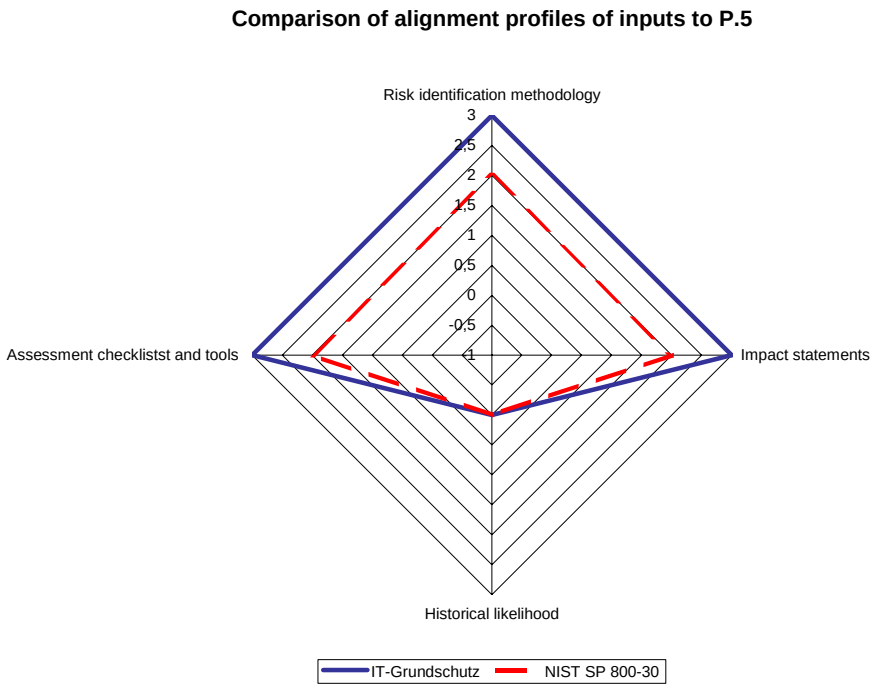

Figure 13: Comparison of alignment profiles of inputs to P.5 for IT-Grundschutz and NIST

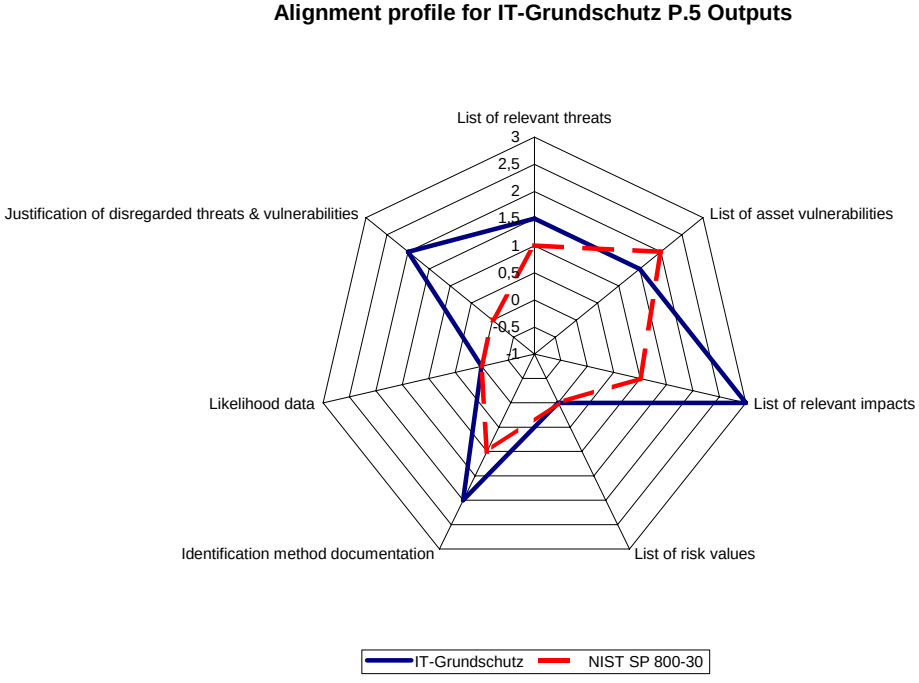

Figure 14: Comparison of alignment profiles of outputs from P.5 for IT-Grundschutz and NIST

Organizations will be able to use comparisons, such as those illustrated in figures 13 and 14, to help determine which process from which items are likely to best meet their requirements, as discussed in section 6. In this example, for instance, it is clear that an organization which wished to justify why it had disregarded certain threats and vulnerabilities would have to use IT-Grundschutz for process P.5, in preference to NIST.

References

[BSI1] BSI Standard 100-1: "Information Security Management Systems", Bundesamt für Sicherheit in der Informationstechnik,version 1.0, December 2005, http://www.bsi.bund.de/english/publications/bsi_standards

[BSI2] BSI Standard 100-2: "IT-Grundschutz Methodology", Bundesamt für Sicherheit in der Informationstechnik, version 1.0, December 2005, http://www.bsi.bund.de/english/publications/bsi_standards

[BSI3] BSI-Standard 100-3: "Risk Analysis based on IT-Grundschutz ", Bundesamt für Sicherheit in der Informationstechnik, version 2.0, December 2005, http://www.bsi.bund.de/english/publications/bsi_standards

[DAK] 'Handleiding Afhankelijkheids- en Kwetsbaarheidsanalyse: stappenplan voor de uitvoering van een A&K-analyse' (in Dutch), version 1.01, Ministry of Internal Affairs, The Hague, 1996, The Netherlands

[ISO] ISO/IEC 17799:2005, Information technology- Security techniques – code of practice for information security management, version 2005, ISO, http://www.iso.ch

[NIST] NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology, July 2002, http://csrc.nist.gov/publications/nistpubs/

Annex A - Benchmark for risk assessment and management processes, inputs and outputs

Stage	Process	Input	Output
A. Definition of scope and framework	P.1 Definition of external environment	I.1.1 Market information (market indicators, competitive information, etc.) I.1.2 Financial & political information I.1.3 Relevant legal and regulatory information I.1.4 Information about geographical, social and cultural conditions I.1.5 Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)	O.1.1 All records of the external environment of the organization O.1.2 List of relevant obligatory laws and regulations (with respect to obligations) O.1.3 Various lists with applicable rules (social, cultural, values etc.)
	P.2 Definition of internal environment	I.2.1 Strategy on the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structure) I.2.2 Description of internal stakeholders I.2.3 Assets in terms of resources (people, systems, processes, capital, etc.)	O.2.1 Description of internal roles (and responsibilities) O.2.2 Description of the main business processes O.2.3 Description of internal assets (e.g. computing center, cooling system, heating system, network, etc.) O.2.4 Description of relationships between O.2.2 and O.2.3 O.2.5. List of strategies (including IT-Strategy and IT-security strategy, if existing) O.2.6 Risk appetite or tolerance (risk orientation of the organization)

Stage	Process	Input	Output
	P.3 Generation of risk management context	I.3.1 O.2.3 I.3.2 Target object scope I.3.3 Scope of the assessment/ management activities (inclusion/exclusion of parts) I.3.4 Definition of roles involved in the assessment/management activity I.3.5 Dependencies with other activities and, processes	O.3.1 Detailed assessment/management plan including: O.3.2 List of assigned participants to roles in the assessment/ management activities O.3.3 List of other activities and actions to be taken under consideration (e.g. cooperation, interfacing etc.) O.3.4 Definition of the organization and process to be assessed
	P.4 Formulation of impact limit criteria	I.4.1 Rules for impact acceptance including frequency, severity and value of assets affected I.4.2 Asset classification reflecting the importance/value of assets to the business	O.4.1 List with criteria for the forthcoming assessment activities O.4.2 Classification scheme for assets
B. Risk assessment	P.5 Identification of risks	I.5.1 Determined methodology to be used for the identification of risk (i.e. threats, vulnerabilities and impacts) I.5.2 Threats, vulnerabilities and impact statements that will be used in the assessment I.5.3 Historical information that can be used to assess the likelihood of impact I.5.4 Checklists and tools for the assessment	O.5.1 List of relevant threats O.5.2 List of relevant vulnerabilities of (groups of) assets O.5.3 List of relevant impacts O.5.4 List of values including frequency, severity and value of assets affected O.5.5 Documentation of the identification method O.5.6 Likelihood data (e.g. history database) O.5.7 Justification for threats and vulnerabilities intentionally disregarded

Stage	Process	Input	Output
	P.6 Analysis of relevant risks	I.6.1 All outputs from 5 above I.6.2 Lists with relevant detailed assets (drawn from O.2.4) I.6.3 O.5.1 with information about risk limits and O.4.2 I.6.4 List of existing controls (technical / organizational)	O.6.1 Tables with assets classified according to the classification scheme O.6.2 List of threats and vulnerabilities relative to each asset O.6.3 List of existing controls relative to each asset (part of so-called gap analysis) O.6.4 List of impacts relative to each asset O.6.5 List of risks relative to each asset O.6.6 (According to the analysis method) Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group)
	P.7 Evaluation of risks	I.7.1 All outputs of 6 above I.7.2 All outputs of 4	O.7.1 Formal decision by Management about previously analyzed risks and about which risks will be treated (and possibly with what priority) or left untreated
C. Risk treatment	P.8 Identification of options	I.8.1 O.4.1 including the relevant limits for the risks I.8.2 O.7.1 I.8.3 List of options for risk treatment	O.8.1 Risk treatment options according to risks (possibly classified according to the risk limits)
	P.9 Development of action plan	I.9.1 O.8.1 I.9.2 Assigned organizational roles (e.g. from O.3.2) I.9.3 Possible planning methodology I.9.4 Possible priority scheme to be used	O.9.1 Action plan as sequence of prioritized activities (expressed as implementation of controls or as protection of assets) O.9.2 Assignment of resources (e.g. costs) for action plan implementation O.9.3 Assignment of responsibilities for each action
	P.10 Approval of action plan	I.10.1 O.9.1 I.10.2 Reports and presentation techniques for findings of I.10.1	O.10.1 Approved lists with activities

Stage	Process	Input	Output
	P.11 Implementation of action plan	I.11.1 O.9.1 I.11.2 O.3.3 I.11.3 Reporting scheme from within other activities I.11.4 Reporting on costs for implementation	O.11.1 Coordination of activities O.11.2 Progress reports from other projects O.11.3 Progress reports from the implementation of measurements (e.g. from ISMS) O.11.4 Overview of costs
	P.12 Identification of residual risks	I.12.1 O.14.1	O.12.1 Triggering of activities 6 and 7 O.12.2 Evaluated residual risks
D. Risk acceptance	P.13 Risk acceptance	I.13.1 O.12.2 I.13.2 O.7.1	O.13.1 Formal decision by management on the way risks have been treated
E. Monitor and Review	P.14 Risk monitoring and reporting	I.14.1 External reference documents e.g.: - Metrics methodologies - Incident data from CERTs - Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.) I.14.2 Internal reference documents: - O.7.1, O.13.1 - O.11.3 I.14.3 Lists of Security Policies I.14.4 O.9.1 I.14.5 Reports on incidents from business processes I.14.6 O.9.2 (concerning costs)	O.14.1 Reports on events and consequences to internal stakeholders O.14.2 Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders) O.14.5 Internal indicators (e.g. KPIs) O.14.6 Cost indicators
F. Risk communication awareness and consulting	P.15 Risk communication, awareness and consulting	I.15.1 Reporting on incidents (external and internal) I.15.2 Requests to inform Management arising from the risk treatment plan I.15.3 Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems) I.15.4 Consulting reports from experts (internal and external) I.15.5 Requests for consulting on detailed security issues, or to perform an evaluation activity.	O.15.1 Communication to internal and external partners O.15.2 Awareness information for all involved stakeholders O.15.3 Consulting request to external specialists O.15.4 Risk communication plan for the enterprise.

Annex B - Mapping the Benchmark to specific items

Mapping the Benchmark to ISO 17799:2005 ([ISO])

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
A. Definition of scope and framework	P.1 Definition of external environment	1	I.1.1 Market information (market indicators, competitive information, etc.)	Absent	0	O.1.1 All records of the external environment of the organization	Absent	0
			I.1.2 Financial & political information	Absent	0	O.1.2 List of relevant obligatory laws and regulations (with respect to obligations)	15.1.1 Identification of applicable legislation	1
			I.1.3 Relevant legal and regulatory information	15.1 Compliance with legal requirements	1.5	O.1.3 Various lists with applicable rules (social, cultural, values etc.)	15.1.1 Identification of applicable legislation	1
			I.1.4 Information about geographical, social and cultural conditions	6.1.6 Contact with authorities	1			
			I.1.5 Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 6.2.1 Identification of risks related	1.5			

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
				to external parties				
	P.2 Definition of internal environment	1	I.2.1 Strategy on the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structure)	5.1.1 Information security policy document 6.1.1 Management commitment to information security	1.5	O.2.1 Description of internal roles (and responsibilities)	8.1.1 Roles and responsibilities	1,5
			I.2.2 Description of internal stakeholders	6.1.2 Information security co-ordination 6.1.3 Allocation of information security responsibilities	1.5	O.2.2 Description of the main business processes	Absent	0
			I.2.3 Assets in terms of resources (people, systems, processes, capital, etc.)	7.1.1 Inventory of assets	1.5	O.2.3 Description of internal assets (e.g. computing centre, cooling system, heating system, network, etc.)	9.2 Equipment security	1,5
						O.2.4 Description of relationships between O.2.2 and O.2.3	7.2 Information classification	1,5
						O.2.5. List of strategies (including IT-Strategy and IT-security strategy, if existing)	5.1.1 Information security policy document	1,5

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
						O.2.6 Risk appetite or tolerance (risk orientation of the organization)	4.1 Assessing security risks	1
	P.3 Generation of risk management context	1.5	I.3.1 O.2.3	9.2 Equipment security	1.5	O.3.1 Detailed assessment/management plan including:	6.1.1 Management commitment to information security	1
			I.3.2 Target object scope	4.1 Assessing security risks	1	O.3.2 List of assigned participants to roles in the assessment/ management activities	6.1.3 Allocation of information security responsibilities	1,5
			I.3.3 Scope of the assessment/ management activities (inclusion/exclusion of parts)	5.1.1. Information security policy document	1	O.3.3 List of other activities and actions to be taken under consideration (e.g. cooperation, interfacing etc.)	6.1.5 Confidentiality agreements 6.1.6 Contact with authorities 6.1.7 Contact with special interest groups	1,5
			I.3.4 Definition of roles involved in the assessment/management activity	6.1.3 Allocation of information security responsibilities	1.5	O.3.4 Definition of the organization and process to be assessed	5.1.1. Information security policy document	1
			I.3.5 Dependencies with other activities and, processes	Absent	0			

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
	P.4 Formulation of impact limit criteria	1	I.4.1 Rules for impact acceptance including frequency, severity and value of assets affected	4.2 Treating security risks	1	O.4.1 List with criteria for the forthcoming assessment activities	Absent	0
			I.4.2 Asset classification reflecting the importance/value of assets to the business	7.2 Information classification	1.5	O.4.2 Classification scheme for assets	7.2.1 Classification guidelines	1,5
B. Risk assessment	P.5 Identification of risks	0.5	I.5.1 Determined methodology to be used for the identification of risk (i.e. threats, vulnerabilities and impacts)	4.1 Assessing security risks (reference to ISO/IEC TR 13335-3)	1	O.5.1 List of relevant threats	Absent	0
			I.5.2 Threats, vulnerabilities and impact statements that will be used in the assessment	Absent	0	O.5.2 List of relevant vulnerabilities of (groups of) assets	Absent	0
			I.5.3 Historical information that can be used to assess the likelihood of impact	5.1.2 Review of the information security policy	1	O.5.3 List of relevant impacts	Absent	0
			I.5.4 Checklists and tools for the assessment	Absent	0	O.5.4 List of values including frequency, severity and value of assets affected	Absent	0
						O.5.5 Documentation of the identification method	Absent	0
						O.5.6 Likelihood data (e.g. history database)	Absent	0
						O.5.7 Justification for	Absent	0

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
						threats and vulnerabilities intentionally disregarded		
	P.6 Analysis of relevant risks	1	I.6.1 All outputs from 5 above	Absent	0	O.6.1 Tables with assets classified according to the classification scheme	7.1.1 Inventory of assets	1
			I.6.2 Lists with relevant detailed assets (drawn from O.2.4)	7.2 Information classification	1.5	O.6.2 List of threats and vulnerabilities relative to each asset	7.1.1 Reference to ISO/IEC TR 13335-3	1
			I.6.3 O.5.1 with information about risk limits and O.4.2	4.1 Assessing security risks (reference to ISO/IEC TR 13335-3) 7.2 Information classification	1	O.6.3 List of existing controls relative to each asset (part of so-called gap analysis)	7.1.1 Reference to ISO/IEC TR 13335-3	1
			I.6.4 List of existing controls (technical / organizational)	4.2 Treating security risks	1	O.6.4 List of impacts relative to each asset	7.1.1 Reference to ISO/IEC TR 13335-3	1
						O.6.5 List of risks relative to each asset	7.1.1 Reference to ISO/IEC TR 13335-3	1
						O.6.6 (According to the analysis method) Qualified or quantified risks	7.1.1 Reference to ISO/IEC TR 13335-3	1

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
						relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group)		
	P.7 Evaluation of risks	1	I.7.1 All outputs of 6 above	7.1.1 Reference to ISO/IEC TR 13335-3	1	O.7.1 Formal decision by Management about previously analyzed risks and about which risks will be treated (and possibly with what priority) or left untreated	6.1.1 Management commitment to information security	1
			I.7.2 All outputs of 4		0.75			
C. Risk treatment	P.8 Identification of options	1	I.8.1 O.4.1 including the relevant limits for the risks		0	O.8.1 Risk treatment options according to risks (possibly classified according to the risk limits)	4.2 Treating security risks	1
			I.8.2 O.7.1		1			
			I.8.3 List of options for risk treatment	4.2 Treating security risks	1			
	P.9 Development of action plan	2	I.9.1 O.8.1		1	O.9.1 Action plan as sequence of prioritized activities (expressed as	4.2 Treating security risks	1

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
						implementation of controls or as protection of assets)		
			I.9.2 Assigned organizational roles (e.g. from O.3.2)	6.1.3 Allocation of information security responsibilities	1.5	O.9.2 Assignment of resources (e.g. costs) for action plan implementation	4.2 Treating security risks	1
			I.9.3 Possible planning methodology	4.2 Treating security risks	1	O.9.3 Assignment of responsibilities for each action	6.1.3 Allocation of information security responsibilities	1
			I.9.4 Possible priority scheme to be used	4.2 Treating security risks	1			
	P.10 Approval of action plan	1	I.10.1 O.9.1		1	O.10.1 Approved lists with activities	6.1.3 Allocation of information security responsibilities	1
			I.10.2 Reports and presentation techniques for findings of I.10.1	6.1.2 Information security coordination	1			
	P.11 Implementation of action plan	2	I.11.1 O.9.1		1	O.11.1 Coordination of activities	6.1.2 Information security coordination	1
			I.11.2 O.3.3		1.5	O.11.2 Progress reports from other projects	5.1.2 Review of the information security policy	1

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.11.3 Reporting scheme from within other activities	6.1.2 Information security coordination	1	O.11.3 Progress reports from the implementation of measurements (e.g. from ISMS)	5.1.2 Review of the information security policy	1
			I.11.4 Reporting on costs for implementation	4.2 Treating security risks	1	O.11.4 Overview of costs	4.2 Treating security risks	1
	P.12 Identification of residual risks	1	I.12.1 O.14.1		1	O.12.1 Triggering of activities 6 and 7	5.1.2 Review of the information security policy	1
						O.12.2 Evaluated residual risks	Absent	0
D. Risk acceptance	P.13 Risk acceptance	1	I.13.1 O.12.2		0	O.13.1 Formal decision by management on the way risks have been treated	5.1.2 Review of the information security policy 6.1.1 Management commitment to information security	1,5
			I.13.2 O.7.1		1			
E. Monitor and review	P.14 Risk monitoring and reporting	1.5	I.14.1 External reference documents e.g.: - Metrics methodologies - Incident data from CERTs - Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.)	6.1.7 Contact with special interest groups	1	O.14.1 Reports on events and consequences to internal stakeholders	6.1.2 Information security coordination	1

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.14.2 Internal reference documents: - O.7.1, O.13.1 - O.11.3		1.17	O.14.2 Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders)	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 6.2 External parties	1,5
			I.14.3 Lists of Security Policies	5.1.1 Information security policy document	1	O.14.3 Internal indicators (e.g. KPIs)	5.1.2 Review of the information security policy	1
			I.14.4 O.9.1		1	O.14.4 Cost indicators	Absent	0
			I.14.5 Reports on incidents from business processes	13.1.1 Reporting information security events	1.5			
			I.14.6 O.9.2 (concerning costs)		1			
F. Risk communication, awareness and consulting	P.15 Risk communication, awareness and consulting	2	I.15.1 Reporting on incidents (external and internal)	13.1 Reporting information security events and weaknesses	2	O.15.1 Communication to internal and external partners	6.1.2 Information security coordination 6.2.2 Addressing security when dealing with customers 6.2.3 Addressing security in third party agreements	2
			I.15.2 Requests to inform Management arising from the risk treatment plan	5.1.2 Review of the information security policy	1	O.15.2 Awareness information for all involved stakeholders	8.2.2 Information security awareness,	1,5

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
				6.1.1 Management commitment to infrmation security			education, and training	
			I.15.3 Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems)	8.2.2 Information security awareness, education and training	1.5	O.15.3 Consulting request to external specialists	6.1.7 Contact with special interest groups	1,5
			I.15.4 Consulting reports from experts (internal and external)	6.1.8 Independent review of information security 15.2 Compliance with security policies and standards, and technical compliance 15.3.1 Information systems audit controls	2	O.15.4 Risk communication plan for the enterprise	6.1.2 Information security coordination	1
			I.15.5 Requests for consulting on detailed security issues, or to perform an evaluation activity.	6.1.7 Contact with special interest groups 6.1.8 Independent review of information security	1.5			

Mapping the Benchmark to the IT-Grundschutz methodology ([BSI1], ([BSI2], ([BSI3])

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
A. Definition of scope and framework	P.1 Definition of external environment	1	I.1.1 Market information (market indicators, competitive information, etc.) I.1.2 Financial & political information I.1.3 Relevant legal and regulatory information I.1.4 Information about geographical, social and cultural conditions I.1.5 Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)	I.1.1. BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) I.1.2. BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) I.1.3 BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) I.1.4 BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) I.1.5 (0)	O.1.1 All records of the external environment of the organization O.1.2 List of relevant obligatory laws and regulations (with respect to obligations) O.1.3 Various lists with applicable rules (social, cultural, values etc.)	O.1.1 BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) O.1.2 BSI Standard 100-2 §3.1.1 Determining the environmental conditions (1) O.1.3 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.2 Definition of internal environment	3	I.2.1 Strategy on the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structure) I.2.2 Description of internal stakeholders I.2.3 Assets in terms of resources (people, systems, processes, capital, etc.)	I.2.1 BSI Standard 100-2 §3.1.2 Formulate General IT Security Objectives (3) I.2.2 BSI Standard 100-2 §3.1.2 Formulate General IT Security Objectives (3) I.2.3 BSI Standard 100-2 §3.1.2 Formulate General IT Security Objectives (3)	O.2.1 Description of internal roles (and responsibilities) O.2.2 Description of the main business processes O.2.3 Description of internal assets (e.g. computing centre, cooling system, heating system, network, etc.) O.2.4 Description of relationships between O.2.2 and O.2.3 O.2.5. List of strategies (including IT-Strategy and IT-security strategy, if existing) O.2.6 Risk appetite or tolerance (risk orientation of the organization)	O.2.1 BSI-Standard 100-2 § 3.2 Setting Up an IT Security Organisation (3) O.2.2 BSI-Standard 100-2 § 3.1.3 Drawing up an information security policy (2) O.2.3 BSI-Standard 100-2 § 4.1.1 Documenting the IT Assets §4.1.2 Preparing a Network Plan §4.1.3 Collecting Information on the IT Systems §4.1.4 Collecting Information about the IT Applications and Related Information §4.1.5 Documenting the Rooms (3) O.2.4 BSI-Standard 100-2 §4 4.1 IT Structure Analysis (3) O.2.5 (0) O.2.6 BSI Standard 100-2 §3.1.2 Formulate General IT Security Objectives (3)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.3 Generation of risk management context	3	I.3.1 O.2.3 I.3.2 Target object scope I.3.3 Scope of the assessment/ management activities (inclusion/exclusion of parts) I.3.4 Definition of roles involved in the assessment/management activity I.3.5 Dependencies with other activities and, processes	I.3.1 BSI-Standard 100-2 § 4.1.1 Documenting the IT Assets (3) I.3.2 BSI 100-2 §3.1.3 Drawing up an information security policy (3) I.3.4. BSI 100-2 §3.2 Setting up an IT security organization (3) I.3.5. BSI 100-2 §3.2 Setting up an IT security organization, "Co-operation and communication", "IT coordination committee" (2)	O.3.1 Detailed assessment/management plan including: O.3.2 List of assigned participants to roles in the assessment/ management activities O.3.3 List of other activities and actions to be taken under consideration (e.g. cooperation, interfacing etc.) O.3.4 Definition of the organization and process to be assessed	O.3.1. BSI 100-2 § 4.2 Defining Protection Requirements, §4.4 Basic Security Check (3) O.3.2. BSI 100-2 §3.2 Setting up an IT security organization (2) O.3.3 BSI 100-2 § 3.1.3 Drawing up an information security policy (1,5) O.3.4 BSI 100-2 § 3.1.2 Formulate general IT Security Objectives (content: general business processes security requirements assessment) (2,5)
	P.4 Formulation of impact limit criteria	3	I.4.1 Rules for impact acceptance including frequency, severity and value of assets affected I.4.2 Asset classification reflecting the importance/value of assets to the business	I.4.1. BSI 100-2 § 4.2 Defining Protection Requirements, "Defining protection requirements categories" (2,5) I.4.2. BSI 100-2 § 4.2 Defining Protection Requirements (3)	O.4.1 List with criteria for the forthcoming assessment activities O.4.2 Classification scheme for assets	O.4.1. BSI 100-2 § 4.2 Defining Protection Requirements, §4.5 Integrating the Supplementary Security Analysis in the IT-Grundschutz Approach (3) O.4.2. BSI 100-2 § 4.2 Defining Protection Requirements (3)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
B. Risk assessment	P.5 Identification of risks	2,5	I.5.1 Determined methodology to be used for the identification of risk (i.e. threats, vulnerabilities and impacts) I.5.2 Threats, vulnerabilities and impact statements that will be used in the assessment I.5.3 Historical information that can be used to assess the likelihood of impact I.5.4 Checklists and tools for the assessment	I.5.1 BSI 100-2 §4.3.2 Modelling IT Assets, BSI 100-2 §4.5 Integrating the Supplementary Security Analysis in the IT-Grundschutz Approach, BSI 100-3 §4 Determination of additional threats (3) I.5.2 Modules in the IT-Grundschutz Catalogues (3) I.5.3 (0) I.5.4 Modules in the IT-Grundschutz Catalogues, Cross reference tables, GSTOOL (3)	O.5.1 List of relevant threats O.5.2 List of relevant vulnerabilities of (groups of) assets O.5.3 List of relevant impacts O.5.4 List of values including frequency, severity and value of assets affected O.5.5 Documentation of the identification method O.5.6 Likelihood data (e.g. history database) O.5.7 Justification for threats and vulnerabilities intentionally disregarded	O.5.1. Modules in the IT-Grundschutz Catalogues (1,5) O.5.2. Modules in the IT-Grundschutz Catalogues (1,5) O.5.3. Modules in the IT-Grundschutz Catalogues, BSI 100-3 §4 Determination of additional threats (3) O.5.4 (0) O.5.5 BSI 100-3 §4 Determination of additional threats (2) O.5.6 (0) O.5.7. BSI 100-3 §6 Handling risks (2)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.6 Analysis of relevant risks	3	I.6.1 All outputs from 5 above I.6.2 Lists with relevant detailed assets (drawn from O.2.4) I.6.3 O.5.1 with information about risk limits and O.4.2 I.6.4 List of existing controls (technical / organizational)	I.6.2. BSI 100-2 §4.1 IT structure Analysis (3) I.6.3. BSI 100-2 § 4.2 Defining Protection Requirements (3) I.6.4 BSI 100-2 §4.4 Basic Security Check (3)	O.6.1 Tables with assets classified according to the classification scheme O.6.2 List of threats and vulnerabilities relative to each asset O.6.3 List of existing controls relative to each asset (part of so-called gap analysis) O.6.4 List of impacts relative to each asset O.6.5 List of risks relative to each asset O.6.6 (According to the analysis method) Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group)	O.6.1 BSI 100-2 §4.2 Determination of protection requirements (3) O.6.2 BSI 100-2 §4.3.2 Modelling IT Assets, BSI 100-3 §4 Determination of additional threats (2,5) O.6.3 BSI 100-2 §4.4 Basic Security Check (3) O.6.4 BSI 100-2 §4.3.2 Modelling IT Assets, BSI 100-3 §4 Determination of additional threats (2) O.6.5 BSI 100-2 §4.3.2 Modelling IT Assets, BSI 100-3 §4 Determination of additional threats (3) O.6.6 BSI 100-2 §4.3.2 Modelling IT Assets (3)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.7 Evaluation of risks	2,5	I.7.1 All outputs of 6 above I.7.2 All outputs of 4	(3)	O.7.1 Formal decision by Management about previously analyzed risks and about which risks will be treated (and possibly with what priority) or left untreated	O.7.1 BSI 100-2 §4.5 Integrating the Supplementary Security Analysis in the IT-Grundschutz Approach, BSI 100-3 §6 Handling risks (2,5)
C. Risk treatment	P.8 Identification of options	3	I.8.1 O.4.1 including the relevant limits for the risks I.8.2 O.7.1 I.8.3 List of options for risk treatment	I.8.1 BSI 100-2 § 4.2 Defining Protection Requirements (3) I.8.2 (2,5) I.8.3 BSI 100-3 § 6 Handling risks (3)	O.8.1 Risk treatment options according to risks (possibly classified according to the risk limits)	O.8.1 BSI 100-3 § 6 Handling risks (2,5)
	P.9 Development of action plan	3	I.9.1 O.8.1 I.9.2 Assigned organizational roles (e.g. from O.3.2) I.9.3 Possible planning methodology I.9.4 Possible priority scheme to be used	I.9.1 BSI 100-3 § 6 Handling risks (2,5) I.9.2 BSI 100-2 §3.2 Setting up an IT security organization (1,5) I.9.3 BSI 100-2 §4.6 Implementation of IT Security measures (3)	O.9.1 Action plan as sequence of prioritized activities (expressed as implementation of controls or as protection of assets) O.9.2 Assignment of resources (e.g. costs) for action plan implementation O.9.3 Assignment of responsibilities for each action	O.9.1 BSI 100-2 §4.6 Implementation of IT Security measures (3) O.9.2 BSI 100-2 §3.3 Provision of Resources for IT Security, GSTOOL (3) O.9.3 IT-Grundschutz Catalogues, GSTOOL (3)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.10 Approval of action plan	2,5	I.10.1 O.9.1 I.10.2 Reports and presentation techniques for findings of I.10.1	I.10.1 BSI 100-3 § 6 Handling risks (2,5) I.10.2 BSI 100-2 §5.2 Information Flow in the IT Security Process (1)	O.10.1 Approved lists with activities	BSI 100-2 §4.6 Implementation of IT Security measures (3)
	P.11 Implementation of action plan	2,5	I.11.1 O.9.1 I.11.2 O.3.3 I.11.3 Reporting scheme from within other activities I.11.4 Reporting on costs for implementation	I.11.1 BSI 100-3 § 6 Handling risks (2,5) I.11.2 BSI 100-2 § 3.1.2 Formulate general IT Security Objectives (2,5)	O.11.1 Coordination of activities O.11.2 Progress reports from other projects O.11.3 Progress reports from the implementation of measurements (e.g. from ISMS) O.11.4 Overview of costs	O.11.1 BSI 100-2 §5.2 Information Flow in the IT Security Process (1) O.11.2 (0) O.11.3 BSI 100-2 §5.1 Checking the IT Security Process at all Levels (2) O.11.4 BSI 100-2 §5.1 Checking the IT Security Process at all Levels, GSTOOL (2)
	P.12 Identification of residual risks	2	I.12.1 O.14.1		O.12.1 Triggering of activities 6 and 7 O.12.2 Evaluated residual risks	O.12.1 (3) O.12.2 BSI 100-3 §6 Handling risks (2)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
D. Risk acceptance	P.13 Risk acceptance	2	I.13.1 O.12.2 I.13.2 O.7.1	I.13.1 BSI 100-3 §6 Handling risks (2) I.13.2 BSI 100-2 §4.5 Integrating the Supplementary Security Analysis in the IT-Grundschutz Approach, BSI 100-3 §6 Handling risks (2,5)	O.13.1 Formal decision by management on the way risks have been treated	O.13.1 BSI 100-3 §6 Handling risks (2)
E. Monitor and review	P.14 Risk monitoring and reporting	2,5	I.14.1 External reference documents e.g.: - Metrics methodologies - Incident data from CERTs - Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.) I.14.2 Internal reference documents: - O.7.1, O.13.1 - O.11.3	I.14.1 BSI 100-2 §5.2 Information Flow in the IT Security Process (1) I.14.2 BSI 100-2 §5.2 Information Flow in the IT Security Process (2) I.14.3 IT-Grundschutz samples of security policies, IT-Grundschutz security measures (3)	O.14.1 Reports on events and consequences to internal stakeholders O.14.2 Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders) O.14.5 Internal indicators (e.g. KPIs) O.14.6 Cost indicators	O.14.1 BSI 100-2 §5.2 Information Flow in the IT Security Process (2) O.14.2 (0) O.14.5 (0) O.14.6 BSI 100-2 §3.3 Provision of Resources for IT Security, GSTOOL (3)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
			I.14.3 Lists of Security Policies I.14.4 O.9.1 I.14.5 Reports on incidents from business processes I.14.6 O.9.2 (concerning costs)	I.14.4 BSI 100-2 §4.6 Implementation of IT Security measures (3) I.14.5 BSI 100-2 §5.2 Information Flow in the IT Security Process, IT-Grundschutz Module "Incident handling" (3) I.14.6 BSI 100-2 §3.3 Provision of Resources for IT Security, GSTOOL (3)		

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
F. Risk communication, awareness and consulting	P.15 Risk communication, awareness and consulting	2	I.15.1 Reporting on incidents (external and internal) I.15.2 Requests to inform Management arising from the risk treatment plan I.15.3 Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems) I.15.4 Consulting reports from experts (internal and external) I.15.5 Requests for consulting on detailed security issues, or to perform an evaluation activity.	I.15.1 IT-Grundschutz Module 1.8 “Incident handling” (3) I.15.2 BSI 100-2 §5.1 Checking the IT Security Process at all Levels (2) I.15.3 IT-Grundschutz Module 1.13 “IT security awareness and training” (3) I.15.4 BSI 100-2 §5.2 Information Flow in the IT Security Process (1) I.15. BSI 100-3 §5 4 Determination of additional threats (1)	O.15.1 Communication to internal and external partners O.15.2 Awareness information for all involved stakeholders O.15.3 Consulting request to external specialists O.15.4 Risk communication plan for the enterprise.	O.15.1 BSI 100-2 §5.2 Information Flow in the IT Security Process (2) O.15.2 IT-Grundschutz Module 1.13 “IT security awareness and training” (3) O.15.3 BSI 100-3 §5 4 Determination of additional threats (1) O.15.4 BSI 100-2 §5.2 Information Flow in the IT Security Process (1)

Annex C Mapping the Benchmark to the NIST SP 800-30 methodology ([NIST])

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
A. Definition of scope and framework	P.1 Definition of external environment	(0)	I.1.1 Market information (market indicators, competitive information, etc.) I.1.2 Financial & political information I.1.3 Relevant legal and regulatory information I.1.4 Information about geographical, social and cultural conditions I.1.5 Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)	I.1.1 (0) I.1.2 (0) I.1.3 (0) I.1.4 (0) I.1.5 (0)	O.1.1 All records of the external environment of the organization O.1.2 List of relevant obligatory laws and regulations (with respect to obligations) O.1.3 Various lists with applicable rules (social, cultural, values etc.)	O.1.1 (0) O.1.2 (0) O.1.3 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.2 Definition of internal environment	System characterization (2)	I.2.1 Strategy on the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structure) I.2.2 Description of internal stakeholders I.2.3 Assets in terms of resources (people, systems, processes, capital, etc.)	I.2.1 (0) I.2.2 (0) I.2.3 Chapter 3.1: System related information (hardware, software, system interfaces, data and information, people, functional requirements) (1)	O.2.1 Description of internal roles (and responsibilities) O.2.2 Description of the main business processes O.2.3 Description of internal assets (e.g. computing centre, cooling system, heating system, network, etc.) O.2.4 Description of relationships between O.2.2 and O.2.3 O.2.5. List of strategies (including IT-Strategy and IT-security strategy, if existing) O.2.6 Risk appetite or tolerance (risk orientation of the organization)	O.2.1 Chapter 3.1: System related information (1) O.2.2 (0) O.2.3 Chapter 3.1: System related information (1) O.2.4 (0) O.2.5 (0) O.2.6 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.3 Generation of risk management context	System characterization (2)	I.3.1 O.2.3 I.3.2 Target object scope I.3.3 Scope of the assessment/ management activities (inclusion/exclusion of parts) I.3.4 Definition of roles involved in the assessment/management activity I.3.5 Dependencies with other activities and, processes	I.3.1 O.2.3 (1) I.3.2 Chapter 3.1: System related information (1) I.3.3 Chapter 3.1: System related information (1) I.3.4. Chapter 3.1: System related information (1) I.3.5. (0)	O.3.1 Detailed assessment/management plan including: O.3.2 List of assigned participants to roles in the assessment/ management activities O.3.3 List of other activities and actions to be taken under consideration (e.g. cooperation, interfacing etc.) O.3.4 Definition of the organization and process to be assessed	O.3.1. O.3.2. (0) O.3.3 (0) O.3.4 Chapter 3.1: System related information (1)
	P.4 Formulation of impact limit criteria	System characterization (2)	I.4.1 Rules for impact acceptance including frequency, severity and value of assets affected I.4.2 Asset classification reflecting the importance/value of assets to the business	I.4.1. Chapter 3.1: System related information (1) I.4.2 Chapter 3.1: System related information (1)	O.4.1 List with criteria for the forthcoming assessment activities O.4.2 Classification scheme for assets	O.4.1. (0) O.4.2. Chapter 3.7.1: Risk level matrix (2)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
B. Risk assessment	P.5 Identification of risks	Threat identification (2) Vulnerability identification (2) Likelihood determination (2) Impact analysis (2)	I.5.1 Determined methodology to be used for the identification of risk (i.e. threats, vulnerabilities and impacts) I.5.2 Threats, vulnerabilities and impact statements that will be used in the assessment I.5.3 Historical information that can be used to assess the likelihood of impact I.5.4 Checklists and tools for the assessment	I.5.1 Chapter 3.7: Risk determination (2) I.52 Chapter 3.2: Threat identification (2) Chapter 3.3: Vulnerability identification (2) Chapter 3.5: Likelihood determination (2) Chapter 3.6: Impact analysis (2) I.5.3 (0) I.5.4 Appendices A-C (2)	O.5.1 List of relevant threats O.5.2 List of relevant vulnerabilities of (groups of) assets O.5.3 List of relevant impacts O.5.4 List of values including frequency, severity and value of assets affected O.5.5 Documentation of the identification method O.5.6 Likelihood data (e.g. history database) O.5.7 Justification for threats and vulnerabilities intentionally disregarded	O.5.1. Chapter 3.2: Threat identification (1) Chapter 3.5: Likelihood determination (2) O.5.2. Chapter 3.3: Vulnerability identification (1) O.5.3. Chapter 3.6: Impact analysis (1) O.5.4 (0) O.5.5 Chapter 3.7: risk determination (1) O.5.6 (0) O.5.7 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.6 Analysis of relevant risks	Control analysis (2) Impact analysis (2) Risk determination (2)	I.6.1 All outputs from 5 above I.6.2 Lists with relevant detailed assets (drawn from O.2.4) I.6.3 O.5.1 with information about risk limits and O.4.2 I.6.4 List of existing controls (technical / organizational)	I.6.2. Chapter 3.1: System related information (1) I.6.3. O.5.1 and risk level matrix (1) I.6.4 Chapter 3.4: Control analysis (1)	O.6.1 Tables with assets classified according to the classification scheme O.6.2 List of threats and vulnerabilities relative to each asset O.6.3 List of existing controls relative to each asset (part of so-called gap analysis) O.6.4 List of impacts relative to each asset O.6.5 List of risks relative to each asset O.6.6 (According to the analysis method) Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group)	O.6.1 (0) O.6.2 Chapter 3.7.1: Risk level matrix (1,5) O.6.3 Chapter 3.7.1: Risk level matrix (1,5) O.6.4 Chapter 3.7.1: Risk level matrix (1,5) O.6.5 Chapter 3.7.1: Risk level matrix (1,5) O.6. Chapter 3.7.1: Risk level matrix (1,5)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.7 Evaluation of risks	results documentation (2)	I.7.1 All outputs of 6 above I.7.2 All outputs of 4	I.7.1 All outputs of 6 above (1) I.7.2 All outputs of 4 (1)	O.7.1 Formal decision by Management about previously analyzed risks and about which risks will be treated (and possibly with what priority) or left untreated	O.7.1 Chapter 3.9: Results documentation (1,5)
C. Risk treatment	P.8 Identification of options	control recommendation	I.8.1 O.4.1 including the relevant limits for the risks I.8.2 O.7.1 I.8.3 List of options for risk treatment	I.8.1 (0) I.8.2 O.7.1 (1,5) I.8.3 Chapter 4.1: Risk mitigation options (2)	O.8.1 Risk treatment options according to risks (possibly classified according to the risk limits)	O.8.1 Chapter 4.1: Risk mitigation options (2), Risk mitigation strategy (2)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.9 Development of action plan	Prioritize actions (2) Evaluate recommended control options (2) conduct cost-benefit analysis (2) select controls (2) assign responsibilities (2) develop a safeguard implementation plan (2)	I.9.1 O.8.1 I.9.2 Assigned organizational roles (e.g. from O.3.2) I.9.3 Possible planning methodology I.9.4 Possible priority scheme to be used	I.9.1 O.8.1 (2) I.9.2 Chapter 4.3: approach for control implementation (1) I.9.3 (0) I.9.4 (0)	O.9.1 Action plan as sequence of prioritized activities (expressed as implementation of controls or as protection of assets) O.9.2 Assignment of resources (e.g. costs) for action plan implementation O.9.3 Assignment of responsibilities for each action	O.9.1 Chapter 4.3: approach for control implementation, step 6 (1,5) O.9.2 Chapter 4.3: approach for control implementation, step 6 (1,5) O.9.3 Chapter 4.3: approach for control implementation, step 6 (1,5)
	P.10 Approval of action plan	(0)	I.10.1 O.9.1 I.10.2 Reports and presentation techniques for findings of I.10.1	I.10.1 (0) I.10.2 (0)	O.10.1 Approved lists with activities	O.10.1 (0)
	P.11 Implementation of action plan	Implement selected controls (1)	I.11.1 O.9.1 I.11.2 O.3.3 I.11.3 Reporting scheme from within other activities I.11.4 Reporting on costs for implementation	I.11.1 O.9.1 I.11.2 (0) I.11.3 (0) I.11.4 (0)	O.11.1 Coordination of activities O.11.2 Progress reports from other projects O.11.3 Progress reports from the implementation of measurements (e.g. from ISMS) O.11.4 Overview of costs	O.11.1 (0) O.11.2 (0) O.11.3 Chapter 4.3: approach for control implementation, step 7 (1) O.11.4 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
	P.12 Identification of residual risks	residual risk (1)	I.12.1 O.14.1	I.12.1 (0)	O.12.1 Triggering of activities 6 and 7 O.12.2 Evaluated residual risks	O.12.1 ? O.12.2 Chapter 4.6: residual risk (1)
D Risk acceptance	P.13 Risk acceptance	(0)	I.13.1 O.12.2 I.13.2 O.7.1	I.13.1 (0) I.13.2 (0)	O.13.1 Formal decision by management on the way risks have been treated	O.13.1 (0)
E Risk Monitor and Review	P.14 Risk indicator gathering and reporting	(0)	I.14.1 External reference documents e.g.: - Metrics methodologies - Incident data from CERTs - Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.) I.14.2 Internal reference documents: - O.7.1, O.13.1 - O.11.3 I.14.3 Lists of Security Policies I.14.4 O.9.1 I.14.5 Reports on incidents from business processes I.14.6 O.9.2 (concerning costs)	I.14.1 (0) I.14.2 (0) I.14.3 (0) I.14.4 (0) I.14.5 (0) I.14.6 (0)	O.14.1 Reports on events and consequences to internal stakeholders O.14.2 Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders) O.14.5 Internal indicators (e.g. KPIs) O.14.6 Cost indicators	O.14.1 (0) O.14.2 (0) O.14.5 (0) O.14.6 (0)

Stage	Process	Process Score	Benchmark Input	Item Input (Score)	Benchmark Output	Item Output (Score)
F. Risk communication, awareness and consulting	P.15 Risk communication, awareness and consulting	(0)	I.15.1 Reporting on incidents (external and internal) I.15.2 Requests to inform Management arising from the risk treatment plan I.15.3 Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems) I.15.4 Consulting reports from experts (internal and external) I.15.5 Requests for consulting on detailed security issues, or to perform an evaluation activity.	I.15.1 (0) I.15.2 (0) I.15.3 (0) I.15.4 (0) I.15.5 (0)	O.15.1 Communication to internal and external partners O.15.2 Awareness information for all involved stakeholders O.15.3 Consulting request to external specialists O.15.4 Risk communication plan for the enterprise.	O.15.1 (0) O.15.2 (0) O.15.3 (0) O.15.4 (0)

Annex D Mapping the Benchmark to the Dutch A&K Analysis methodology ([DAK])

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
A. Definition of scope and framework	P.1 Definition of external environment	0	I.1.1 Market information (market indicators, competitive information, etc.)		0	O.1.1 All records of the external environment of the organization		0
			I.1.2 Financial & political information		0	O.1.2 List of relevant obligatory laws and regulations (with respect to obligations)		0
			I.1.3 Relevant legal and regulatory information		0	O.1.3 Various lists with applicable rules (social, cultural, values etc.)		0
			I.1.4 Information about geographical, social and cultural conditions		0			
			I.1.5 Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)		0			
	P.2 Definition of internal environment	1.3	I.2.1 Strategy on the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structure)		0	O.2.1 Description of internal roles (and responsibilities)	Part 1,step 3 and 4	2

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.2.2 Description of internal stakeholders	Part 2, step 1: Focus and scope Part 2, step 2: Business processes	2	O.2.2 Description of the main business processes	Part 2, step 2+3: Description of business processes	2
			I.2.3 Assets in terms of resources (people, systems, processes, capital, etc.)	Part 2, step 4: System information (assets, documentation)	2	O.2.3 Description of internal assets (e.g. computing centre, cooling system, heating system, network, etc.)	Part 2, step 4+5: Description of system assets	2
						O.2.4 Description of relationships between O.2.2 and O.2.3	Part 2, step 6: Description of relationships between O.2.2 and O.2.3	2
						O.2.5. List of strategies (including IT-Strategy and IT-security strategy, if existing)		0
						O.2.6 Risk appetite or tolerance (risk orientation of the organization)		0
	P.3 Generation of risk management context	0.7	I.3.1 O.2.3		0	O.3.1 Detailed assessment/management plan including:		0

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.3.2 Target object scope		0	O.3.2 List of assigned participants to roles in the assessment/ management activities	Part 1 ,step 5 and 6	2
			I.3.3 Scope of the assessment/ management activities (inclusion/exclusion of parts)	Part I ,step 5	1	O.3.3 List of other activities and actions to be taken under consideration (e.g. cooperation, interfacing etc.)	Part 1 ,step 5 and 6	2
			I.3.4 Definition of roles involved in the assessment/management activity	Part 1 , step 3	1	O.3.4 Definition of the organization and process to be assessed		0
			I.3.5 Dependencies with other activities and, processes		0			
	P.4 Formulation of impact limit criteria	0.3	I.4.1 Rules for impact acceptance including frequency, severity and value of assets affected	Part 1 ,step 22 to 13	1	O.4.1 List with criteria for the forthcoming assessment activities		0
			I.4.2 Asset classification reflecting the importance/value of assets to the business		0	O.4.2 Classification scheme for assets		0
B. Risk assessment	P.5 Identification of risks	1.5	I.5.1 Determined methodology to be used for the identification of risk (i.e. threats, vulnerabilities and impacts)	Part 1: Description of risk assessment methodology	2	O.5.1 List of relevant threats	Part 2, step 10: List of threats	2

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.5.2 Threats, vulnerabilities and impact statements that will be used in the assessment	Part 2, step 10: Asset, threat and impact lists	2	O.5.2 List of relevant vulnerabilities of (groups of) assets	Part 2, step 9: List of system components	2
			I.5.3 Historical information that can be used to assess the likelihood of impact		0	O.5.3 List of relevant impacts	Part 2, step 10 + 11: List of relevant impacts	2
			I.5.4 Checklists and tools for the assessment	Part 3, appendices : Checklists and examples	2	O.5.4 List of values including frequency, severity and value of assets affected		0
						O.5.5 Documentation of the identification method	Part 3, appendices	2
						O.5.6 Likelihood data (e.g. history database)		0
						O.5.7 Justification for threats and vulnerabilities intentionally disregarded	Part 2, step 11 + 12: selection and justification of controls	2
	P.6 Analysis of relevant risks	2	I.6.1 All outputs from 5 above	Outputs from P.5	2	O.6.1 Tables with assets classified according to the classification scheme	Part 2, step 9: Tables with assets	2
			I.6.2 Lists with relevant detailed assets (drawn from O.2.4)	Lists with relevant detailed assets from O.5.2	2	O.6.2 List of threats and vulnerabilities relative to each asset	Part 3, appendices	2
			I.6.3 O.5.1 with information about risk limits and O.4.2	Outputs from P.5	2	O.6.3 List of existing controls relative to each asset (part of so-called gap analysis)	Part 2, step 8: List of existing controls	2

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.6.4 List of existing controls (technical / organizational)	Part 2, step 8: List of existing controls	2	O.6.4 List of impacts relative to each asset	Part 3, appendices	2
						O.6.5 List of risks relative to each asset	Part 3, appendices	2
						O.6.6 (According to the analysis method) Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group)	Part 3, appendices	2
	P.7 Evaluation of risks	0.7	I.7.1 All outputs of 6 above	All outputs of 6 above (1)	1	O.7.1 Formal decision by Management about previously analyzed risks and about which risks will be treated (and possibly with what priority) or left untreated	Part 2, step 11: Identification of relevant risks	1
			I.7.2 All outputs of 4		0			
C. Risk treatment	P.8 Identification of options	1.5	I.8.1 O.4.1 including the relevant limits for the risks		0	O.8.1 Risk treatment options according to risks (possibly classified according to the risk limits)	Part 2, step 12: List of recommended controls; Part 2, step 13 + 14: Evaluation of controls	2
			I.8.2 O.7.1	O.7.1 (2)	2			

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.8.3 List of options for risk treatment	Part 2, step 12: List of relevant controls (2)	2			
	P.9 Development of action plan	0.4	I.9.1 O.8.1		0	O.9.1 Action plan as sequence of prioritized activities (expressed as implementation of controls or as protection of assets)	Part 1 step 5	1
			I.9.2 Assigned organizational roles (e.g. from O.3.2)		0	O.9.2 Assignment of resources (e.g. costs) for action plan implementation		0
			I.9.3 Possible planning methodology	Part 1 ,step 5	1	O.9.3 Assignment of responsibilities for each action	Part 1 ,step 5 and 6	1
			I.9.4 Possible priority scheme to be used		0			
	P.10 Approval of action plan	0	I.10.1 O.9.1		0	O.10.1 Approved lists with activities		0
			I.10.2 Reports and presentation techniques for findings of I.10.1		0			
	P.11 Implementation of action plan	0	I.11.1 O.9.1		0	O.11.1 Coordination of activities		0
			I.11.2 O.3.3		0	O.11.2 Progress reports from other projects		0

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.11.3 Reporting scheme from within other activities		0	O.11.3 Progress reports from the implementation of measurements (e.g. from ISMS)		0
			I.11.4 Reporting on costs for implementation		0	O.11.4 Overview of costs		0
	P.12 Identification of residual risks	0.7	I.12.1 O.14.1	Outputs of P.6 and O.8.1	0	O.12.1 Triggering of activities 6 and 7		0
						O.12.2 Evaluated residual risks	Part 2, step 13 + 14: Residual risks	2
D. Risk acceptance	P.13 Risk acceptance	0	I.13.1 O.12.2		0	O.13.1 Formal decision by management on the way risks have been treated		0
			I.13.2 O.7.1		0			
E. Monitor and review	P.14 Risk monitoring and reporting	0.3	I.14.1 External reference documents e.g.: - Metrics methodologies - Incident data from CERTs - Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.)	several times especially DR 1,step 13	1	O.14.1 Reports on events and consequences to internal stakeholders		0
			I.14.2 Internal reference documents: - O.7.1, O.13.1 - O.11.3		0	O.14.2 Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders)		0
			I.14.3 Lists of Security Policies		0	O.14.3 Internal indicators (e.g. KPIs)		0

Stage	Process	Process Score	Benchmark Input	Item Input	Input Score	Benchmark Output	Item Output	Output Score
			I.14.4 O.9.1		0	O.14.4 Cost indicators	Part 1,step 12	1
			I.14.5 Reports on incidents from business processes	Part 1, step 13	1			
			I.14.6 O.9.2 (concerning costs)		0			
F Risk communication, awareness and consulting	P.15 Risk communication, awareness and consulting	0	I.15.1 Reporting on incidents (external and internal)		0	O.15.1 Communication to internal and external partners		0
			I.15.2 Requests to inform Management arising from the risk treatment plan		0	O.15.2 Awareness information for all involved stakeholders		0
			I.15.3 Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems)		0	O.15.3 Consulting request to external specialists		0
			I.15.4 Consulting reports from experts (internal and external)		0	O.15.4 Risk communication plan for the enterprise		0
			I.15.5 Requests for consulting on detailed security issues, or to perform an evaluation activity.		0			