ENISA *ad hoc* Working Group on National Risk Management Preparedness

Consolidated Report

Prepared by: Members of the ad-hoc Working Group, ENISA and ExecIA LLP
Version: 1.0
Date: April 2011

Legal notice

Notice must be taken that this publication represents the views and interpretations of the editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

Version Control

Version Number	Date	Prepared by	Comment
0.1	18/01/2011	Jeremy Ward	Initial Draft.
0.2	20/01/2011	Guy Bunker	Draft + Example Test Scenario.
0.3	21/01/2011	Jeremy Ward	Final draft + editing.
0.4	21/01/2011	Guy Bunker	Additional editing.
0.5	24/01/2011	Jeremy Ward	Final editing, submitted draft.
0.6	27/01/2011	Jeremy Ward	Updated following ENISA comments.
0.7	28/01/2011	Guy Bunker	Addition of user guide to spreadsheet for questionnaire analysis + minor edits.
0.8	31/01/2011	Jeremy Ward	Updated following ENISA comments.
0.9	01/02/2011	Jeremy Ward	Further updates following ENISA comments.
0.91	02/02/2011	Jeremy Ward	Minor amendments to wording.
0.92	04/02/2011	Jeremy Ward	Minor amendments.
0.93	22/02/2011	Jeremy Ward	Amendments following final ENISA comments.
0.94	07/03/2011	Jeremy Ward	Amendments following WG comments.
0.95	08/03/2011	Jeremy Ward	Further Amendments following WG comments.
0.96	09/03/2011	Guy Bunker/ Jeremy Ward	Final version for WG approval.
0.97	09/03/2011	Jeremy Ward	Final version incorporating additional comments.
0.98	17/03/2011	Jeremy Ward	Final version with ENISA internal amendments.
1.0	11/04/2011	Louis Marinos	Final version after internal ENISA QA

Contents

Indexes

Index of Figures

Index of Tables

1. Executive Summary

This document presents the outcome of an ENISA Working Group on National Risk Management (NRM) preparedness (see the definitions below). It sets out the elements of a framework for the governance of NRM (see definitions) in relation to a country's Critical Information Infrastructure (CII). As such it deals only with the management of information security risk in those critical information infrastructures, rather than risk management in the broader sense.

The present document has been developed in common by ENISA and Members of the Working Group and has been prepared in this final version by ExecIA LLP. In this process ideas of the Working Group Members, ENISA content and proposals of ExecIA LLP have been compiled into this final deliverable. Both the relevant ENISA activity and the Working Group have been managed by Dr. Louis Marinos (louis.marinos@enisa.europa.eu).

The Working Group identified the relationship between NRM and the management of information security risk in individual CII stakeholder organisations (see definitions). It determined that there are three essential NRM processes that need to be implemented by national governments, as follows:

1. Process 1: Define NRM Policy.
2. Process 2: Coordinate and Support Implementation [of risk management in CII stakeholder organisations].
3. Process 3: Review, Reassess and Report [on NRM].

Each of these three processes is supported by a number of activities; of which the Working Group identified 12. A framework for the governance of NRM is described in detail in relation to these three processes and 12 activities.

The framework for the governance of NRM, as described in this document, is not intended to be used as a blueprint for the creation of a fully functioning NRM programme. However, it is intended to enable governments and other stakeholders in a nation's CII to gain an overview of the elements that are required to build such a programme; and to understand the relationships between these elements.

Questionnaires have been devised which allow governments to assess their strengths and weaknesses in relation to NRM preparedness. Separate questionnaires, given in the document, permit assessment by reference to CII stakeholders both within and outside government. Assessments in the questionnaires use a five-level capability maturity measurement, modelled on that used in the COBIT standard.

The document shows how the framework for the governance NRM can be developed and implemented through the use of a clearly defined workflow. In conjunction with information about inputs, outputs and responsibilities detailed in Annex A, this allows governments to understand the steps required to achieve an effective NRM governance framework.

A clear 9-step process to test NRM preparedness is described. This suggests how a test scenario might be selected, it shows how an appropriate level of capability maturity can be chosen for the test and it outlines the content of a test programme. Scenarios which might be developed into test exercises are also suggested.

A brief report is included on NRM preparedness in four EU countries. This was carried out primarily to test the validity and operability of the questionnaires. It does not, therefore, provide a statistically meaningful assessment of NRM preparedness in those four countries; and certainly not in the EU as

a whole. However, preliminary indications are that there may be a generally lower capability in the review and updating of NRM governance than in policy setting and promoting awareness. It is also likely that there is a wide variation in NRM preparedness across the various EU member states.

In addition to providing an overview of NRM governance, it is proposed that this document may be used in a number of practical ways by national governments. These include to:

- Identify strengths and weaknesses in the implementation of NRM in their country;
- Assist in the development of a framework for the governance of NRM;
- Help the government to assist CII stakeholder organisations in developing their own risk management processes; and
- Assess the country's NRM preparedness through the use of a defined testing process.

Definitions

National Risk Management (NRM): The management of risk to a nation's Critical Information Infrastructure (CII).

CII Stakeholder Organisations include governments, sectoral regulators, telecommunications, Internet service providers and major outsourcers for government information systems.

NRM Preparedness: The degree of a nation's maturity and effectiveness in: establishing a policy framework encouraging risk management in its individual CII stakeholder organisations; supporting the implementation of risk management in those organisations and; monitoring and reviewing risk management and adapting national activities accordingly.

NRM Governance Framework: those processes and activities that need to be performed at national and/or sectoral levels in order to set and maintain NRM preparedness.

2. Introduction

2.1 Background

In conformance with its remit from the European Commission and EU member states, ENISA undertakes a multi-annual programme (MTP) to identify emerging risks and assist in the creation of trust and confidence; this is designated MTP 3 in ENISA's 2010 Work Programme. One task of MTP 3 is the enhancement of national risk management preparedness to assist Critical Information Infrastructure (CII) protection within EU countries: WPK 3.3 in the 2010 Work Programme.

The work will also help with the definition of scenarios that are required as part of pan-European resilience exercises. As such, it will also contribute towards another of ENISA's multi-annual programmes – MTP 1: improving resilience in European e-communication networks. Specifically towards WPK 1.4: empower stakeholders towards a first pan-European exercise.

A Working Group has been set up under the auspices of WPK 3.3; consisting of experts on CII from EU countries. This Working Group has had the task of identifying the essential elements of National Risk Management (NRM) governance that are needed to ensure the preparedness of a country to maintain the resilience of its public electronic networks.

It is important to note that the Working Group has confined itself solely to the consideration of risk management in information infrastructures rather than in a wider sphere; for example finance, transport or utilities. The term "National Risk Management (NRM)" must therefore be read throughout this document in the context of the management of information security risk within national critical information infrastructures.

2.2 Working Group and Deliverables

The Working Group consisted of the following members:

- Manuel de Barros: ANACOM, Portugal.
- Dr. Uwe Jendricke: BSI, Germany.
- Charalampos Koutsouris and Dr. Zoe Nivolianitou: NCSR, IIT, Greece.
- Drs. J.C. Oude Alink: Ministry of Economic Affairs, The Netherlands.
- Rytis Rainys: RRT, Lithuania..
- Prof. Ingrid Schaumueller-Bichl and Alexander Leitner: University of Applied Sciences, Hagenberg, Austria.
- Bjorn Scharin: pts, Sweden
- Pascal Steichen: CIRCL, Luxemburg
- Paul Theron: Thales Group, France
- Marco Fernandez-Gonzalez, *Observer* INFSO, European Commission

ENISA staff managed the Working Group:

- Louis Marinos

The Working Group was charged with the production of a number of deliverables. These are listed below (with their location in this document shown in brackets):

- **Deliverable 1**: description of the content of NRM (contained in Section 4 of this document).
- **Deliverable 2**: questionnaires, based on the description of the content of NRM (see Section 5.1 of this document).
- **Deliverables 3 and 4**: report on use of the questionnaire with EU countries and an analysis of the responses (contained in Section 6 of this document).
- **Deliverable 5**: development of a common framework and guidelines for the development of NRM (contained in Section 5.2 of this document);

- **Deliverable 6**: development of recommendations for testing NRM preparedness (contained in Section 5.3 of this document);
- **Deliverable 7**: incorporation of all the above Deliverables (1 to 6) into a single report, covering the actions of the Working Group and the outcomes of their findings (the entirety of this document).

Open issues and proposals for further work are contained in Section 7. A bibliography is at Section 8.

2.3 Document Purpose, Content and Use Cases

The purpose of this document is to describe the delivery of NRM preparedness through the development of processes, activities and functions associated with NRM and its governance. This document is not intended to be used as a blueprint for the creation of a fully functioning NRM programme. However, it is intended to enable governments and other stakeholders in a nation's CII to gain an overview of the elements that are required to build such a programme; and to understand the relationships between these elements.

In order to achieve this, the document contains a description of the processes and activities that constitute NRM. To assist countries to further enhance their existing NRM preparedness, guidance is given on the development of a framework for governance of NRM. There are also suggestions for processes to test NRM preparedness. In addition, the document contains a brief report on an initial survey of NRM capability maturity in four EU countries.

This document may be used by national governments in a number of ways. These include:

- Use of the questionnaire at Annex C to identify strengths and weaknesses in the implementation of NRM, as perceived by the government.
- Use of the questionnaire at Annex D to identify strengths and weaknesses in the implementation of NRM, as perceived by individual CII stakeholder organisations.
- Use of the workflow at Figure 6 and the description in Section 5.2 to assist in the development of NRM.
- Use of the detailed inputs and outputs to and from the framework for NRM governance, shown in Annex A Table 4, as a check-list to provide more in-depth understanding of the requirements for developing NRM preparedness.
- Use of the detailed inputs and outputs information to and from risk management in individual CII stakeholder organisations, shown in Annex B Table 5, as a check-list to assist in the development of risk management in those organisations.
- Use of the processes shown in Section 5.3 to test NRM preparedness.

2.4 Organisations Participating in NRM

The implementation of NRM within a country relies on the participation of a number of different organisational groups. The participating groups are shown in Table 1. The responsibility of these groups for individual governance activities is indicated in the description of the framework for NRM governance (Section 4, below). The abbreviations shown in Table 1 are also used to indicate responsibilities in Table 4 and Table 5.

Name	Abbreviation
National Government	NG
National Security Institution[1]	NSI
Sector Regulator	SR
Individual (CII stakeholder) Organisation	IO

Table 1: Participating organisations

It should be noted that NRM is primarily the concern of national governments and national security institutions. However, all organisations, whether part of national government or of an individual sector, must attach equal importance to the implementation of risk management within their own organisation.

[1] National Security Institutions, in this context, are those that are concerned with the protection of the national critical information infrastructure; such as the German BSI, the UK CPNI or the French ANSSI. See http://www.enisa.europa.eu/act/sr/nis-brokerage-1/files/deliverables/who-is-who-directory-on-nis-ed.-2009

3. Defining NRM and its Governance

3.1 Background

The importance of the protection of the risk to CII within EU countries has been emphasised by the Commission of the European Communities in its communication: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009) 149). Indeed, important and relevant reports in this area have been published by the Commission, such as: "A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet" (JLS/2008/D1/018).

On a more general level, information security risk management for organisations is a well understood concept and is the subject of an international standard: ISO 27005 (Information security – Security techniques – Information security risk management)[2]. However, the *governance* of information security risk management, particularly in the national context, has not been subject to the same degree of scrutiny and standardisation. The ENISA Working Group has therefore considered the issue of NRM in the light of the efforts of previous ENISA Working Groups on risk assessment and risk management; especially considering risk management processes and activities (see: http://www.enisa.europa.eu/act/rm/working-group).

3.2 NRM Processes

Having considered the congruency of information security risk management and NRM, the current Working Group concluded that there are three essential components to the governance of information security risk management in the context of EU member states. These three elements may be described as follows:

1. The establishment of a policy framework to encourage the use of risk management within CII stakeholder organisations in both public and private sectors within EU countries.
2. The investment by EU countries in measures to support individual CII stakeholder organisations in their implementation of appropriate risk management activities.
3. The ability of EU countries to monitor and review current NRM implementation levels and adapt national activities accordingly.

Each of these elements may be regarded as outlining the function of one of three processes considered essential to NRM. This document identifies these three processes as follows:

1. Process 1 (**P1**): Define policy.
2. Process 2 (**P2**): Coordinate and Support Implementation [of risk management in CII stakeholder organisations].
3. Process 3 (**P3**): Review, Reassess and Report [on NRM].

The ability of a national government to implement these three NRM processes is taken to be the measure of the maturity of that country in terms of its NRM preparedness.

3.3 NRM Processes and Risk Management in CII Stakeholders

It is evident that, alongside these three national processes (P1, P2 and P3), individual CII stakeholders must be able to implement effective risk management within their own organisations. Risk management methods for individual organisations encompass the ability to assess risks associated with specific targets (e.g. information systems, applications or infrastructure components) and then act to manage and mitigate those risks. To do this it is recommended that

[2] Reference number ISO/IEC 27005:2008. Published 15th June 2008.

organisations use a clear iterative process such as the "Plan, Do, Check, Act" (PDCA) cycle[3], see Figure 1 below.

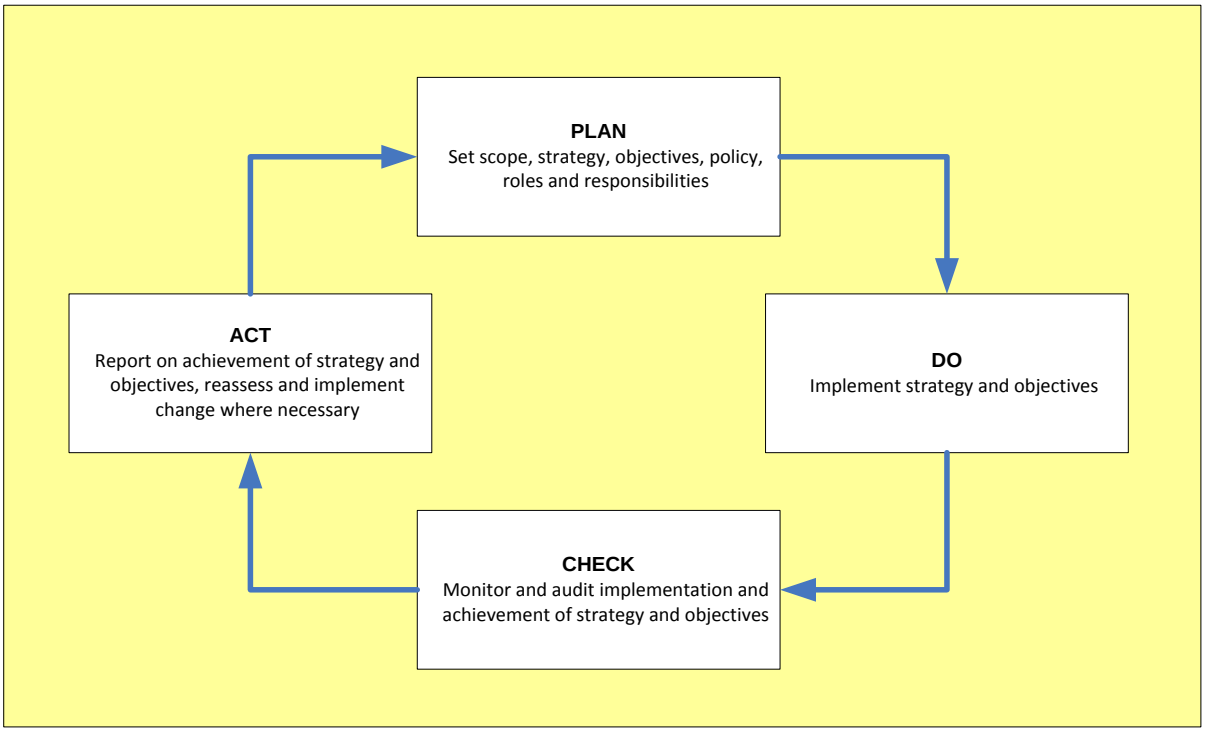

Figure 1: Plan, Do, Check, Act Cycle

The mutual exchange of information between NRM and risk management implementation in individual CII stakeholder organisations is fundamental to the overall management of risk in the national critical information infrastructure. It enables individual CII organisations to manage their risk better; by assisting with coordination of risk response and ensuring consistency and effectiveness of risk management methodologies. Conversely, information received from the risk management implementation process in CII stakeholder organisations ensures that governments have up-to-date information about the management of threats, vulnerabilities and impacts experienced, estimated or perceived by the CII community. Thus governments can steer NRM activities in support of relevant nationwide protection, prevention, detection and response capabilities.

Figure 2, below, shows the relationships and dependencies between the NRM processes (P1, P2 and P3) and risk management implementation in individual CII stakeholder organisations.

[3] As described in ISO/IEC 27001: 2005.

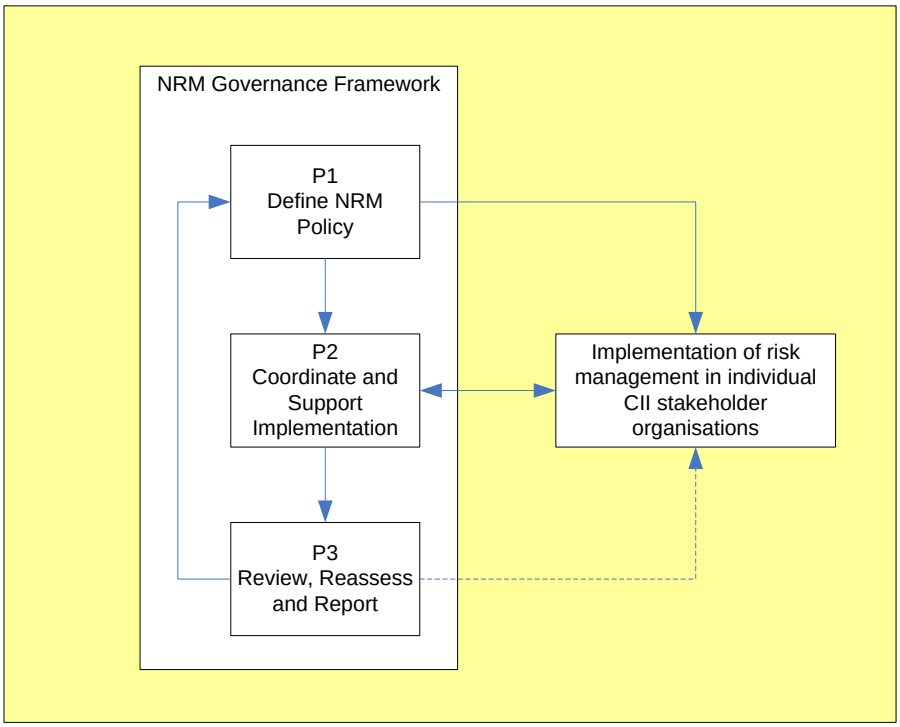

Figure 2: NRM Governance Framework and Risk Management in Individual Organisations

As Figure 2 indicates, the NRM policy definition process (P1) contributes to the implementation of risk management in individual organisations by delivering rules, guidelines and stakeholder coordination information. The NRM process for coordinating and supporting implementation (P2) both contributes to the implementation of risk management in individual CII stakeholder organisations (for example through information sharing) and receives contributions from it (such as information about identified threats, vulnerabilities and impacts).

The review, reassessment and reporting process (P3) does not contribute directly to risk implementation in individual CII stakeholder organisations. However, as Figure 2 indicates through the use of a dotted line, P3 does produce reports on the national governance of risk management that may be issued to individual CII stakeholders for informational purposes.

3.4 NRM Activities and Risk Management Activities in CII Stakeholders

Annex A, Figure 7 and the accompanying Table 4, are a summary of the detailed inputs and outputs for the 12 NRM activities that are described in Section 4, below. The contributory links between NRM activities and risk management activities in CII stakeholder organisations are also described in Section 4. Although the current document does not deal with the implementation of risk management in individual organisations, the processes and activities that form a framework for this are summarised in Annex B. Figure 8 of Annex B shows that risk implementation for individual organisations consists of six processes (labelled P4 to P9 to mesh with the three NRM processes) and eight activities (labelled A13 to A20 to mesh with the 12 NRM activities). Figure 8, and the accompanying Table 5, summarise the inputs and outputs for these processes and activities and indicate their origin and target.

The risk management processes and activities summarised in Annex B are derived from the work of the ENISA Working Group on risk assessment and management, as published in the document "Methodology for evaluating usage and comparison of risk assessment and risk management items", published 26th April 2007. Further information about previous ENISA work in this area may be found on the ENISA website (http://www.enisa.europa.eu/act/rm).

4. The NRM Governance Framework

4.1. Outline of the NRM Governance Framework

The delivery of NRM must take place within a clear governance framework. This framework consists of all the processes and activities that go towards implementing, supporting, coordinating, testing and maintaining NRM. Figure 3, below, is an expansion of the process framework shown in Figure 2; it shows not only the three processes (P1 to P3), but also the activities that form part of NRM (as summarised in Annex A). As can be seen, within the three processes the Working Group has identified 12 activities, shown in the figure as A1 to A12. The content of the three processes and 12 activities is described in detail in sections 4.3, 4.4 and 4.5.

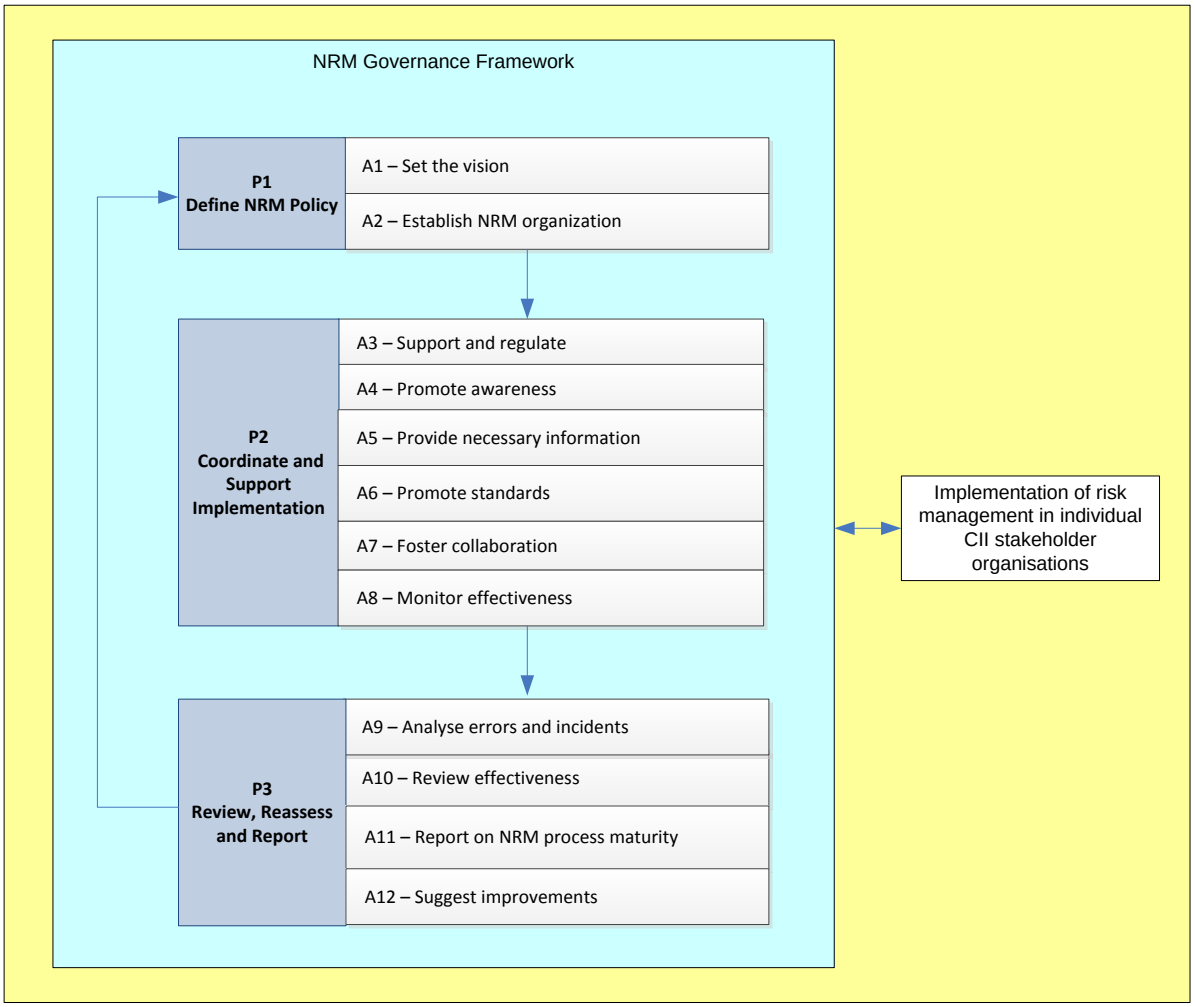

Figure 3: ENISA National Risk Management Activities

The box to the right in Figure 3 once again indicates the interdependency between NRM and risk management in individual CII stakeholder organisations.

In sections 4.3, 4.4 and 4.5 the content of a framework for the governance of NRM is described in detail. The framework is designed to enable organisations to understand the basic elements needed to establish, implement and maintain NRM within their sphere of responsibility.

Each activity is described in relation to other processes and activities that are present not only within NRM, but also within risk management implementation in individual organisations; as well as within other areas such as political, legal and market activity. The description also includes information

about the roles and responsibilities for carrying out each activity. As discussed above, NRM contributes to the implementation of risk management in CII stakeholder organisations. The outputs from each activity forming that contribution are listed; as are the inputs to each NRM activity that are produced by risk management actions within CII stakeholder organisations.

The framework also suggests that National Security Institutions (NSI) (see the definition in footnote 1) assess the strengths and weaknesses of their NRM, by considering the maturity of their capability in each NRM activity. Five clear capability maturity measurement levels have been defined for each activity, based on the five-level model used by the Control Objectives in IT (COBIT) standard[4]. These definitions have been incorporated into a questionnaire, which is given in Annex C. In addition to assessing their own preparedness, the framework shows how governments can determine the strengths and weaknesses of their interaction with CII stakeholder organisations; by considering the maturity of their capability in such interactions in relation to each NRM activity, again modelled on the five-level COBIT capability maturity measurements. A questionnaire for this purpose is given at Annex D.

As part of the framework for implementing governance of NRM, it is intended that NRM activities, like those of information security risk management, should follow an iterative Plan, Do, Check, Act (PDCA) cycle. Figure 4, below, illustrates how the 12 NRM activities fit into a PDCA cycle. Following this cycle should assist governments in implementing or developing their own framework for the governance of NRM. Further guidance can be found in Section 5.2.

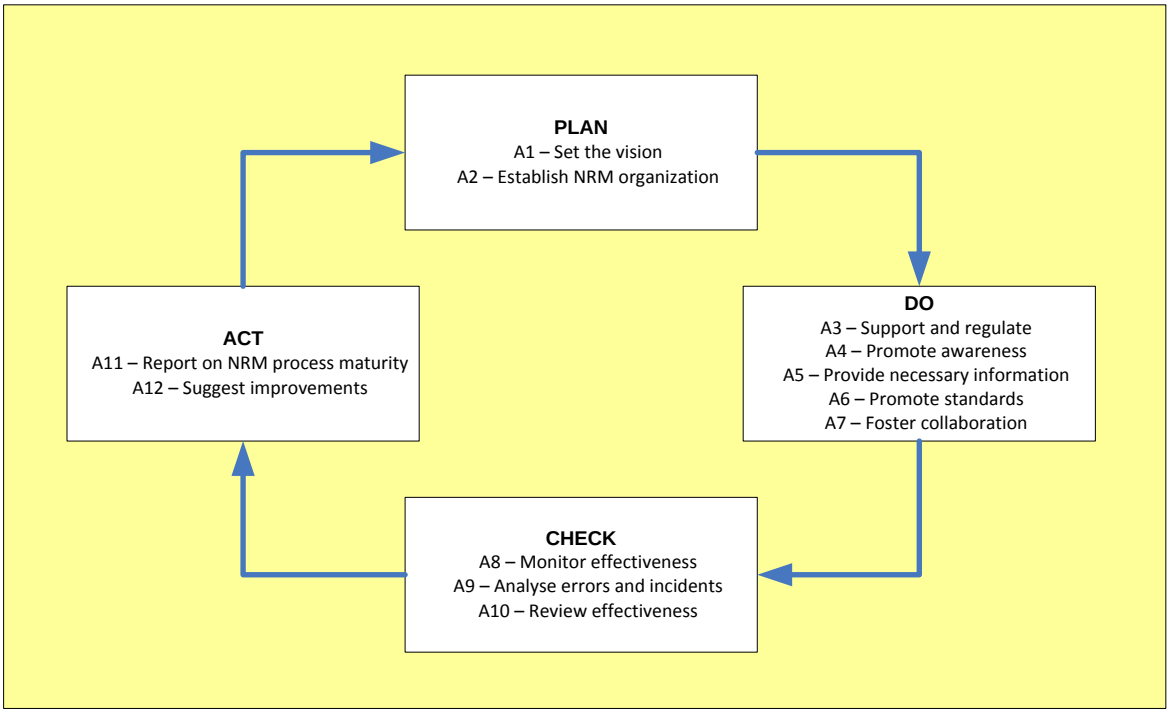

Figure 4: Plan, Do, Check, Act Cycle for NRM Governance Activities

4.2. Structure of the Description of the NRM Governance Framework

The description of the framework for governance of NRM is arranged in three sections (4.3, 4.4 and 4.5), one for each of the three processes (P1, P2 and P3). Each section takes the following form:

- A description of the function of the process.

[4] COBIT 4.1. ISBN 1-933284-72-2. Copyright IT Governance Institute 2007. The model is derived from work by Carnegie Mellon University published in 1993, on behalf of the US Government, aimed at the assessment of software contractors.

- A description of each activity within the process (see Figure 3), containing the following:
  - A narrative description of the activity, its inputs and outputs.
  - A narrative description of the high-level responsibilities for the activity.
  - An overview of the other activities, within the framework, on which the activity depends.
  - A list of the outputs, which will be produced by the NRM activity, for use by CII stakeholder organisations in their risk management implementation. Also of the outputs of CII stakeholder organisations' risk management that will be used by the NRM activity. It is important to note that the names given to these inputs and outputs in this description are indicative only; they may be varied in accordance with the requirements and circumstances of the users of the framework.
  - Links are given to appropriate portions of the questionnaires at Annexes C and D . These contain questions enabling the assessment of NRM strengths and weaknesses by using statements relating to the five levels of capability maturity measurement for both expected NRM preparedness and CII stakeholder expectations. For example, at level 1 capability maturity, the relevant NRM activity would be mostly absent; and a CII stakeholder could expect to receive no help or guidance. Whereas, at level 5 capability maturity, the NRM activity would be fully proactive and highly effective and CII stakeholders could expect to receive detailed guidance that is delivered when required.

4.3. Description of Process 1: Define NRM Policy

This process contains activities concerning the establishment of a policy framework for NRM (including political decisions, relevant laws and regulations). This process is fundamental to NRM governance by setting the context within which it should operate, the strategic goals that it should seek to achieve and the organisation that will enable it to be implemented.

A1: Set the Vision

This activity takes into account political and legal decisions and requirements, as well as current NRM status, effectiveness and activities in relation to the protection of the CII, in order to set strategic goals and objectives for National Risk Management. It identifies key stakeholders and their ability to collaborate and contribute towards NRM outputs including regulation, goal setting and incentives for collaboration.

Responsibilities

National governments have the responsibility for setting NRM policy and strategy and identifying significant CII stakeholders; taking into account the political, legal, regulatory and social conditions in which NRM has to operate.

Dependencies

This activity depends on the delivery of NRM preparedness status reports from activity A11 and of action plans for NRM improvement from activity A12. **Note**: until the NRM governance framework has been fully implemented, activities A11 and A12 will not have been carried out and these reports will therefore not exist.

Inputs to, and outputs from CII stakeholder risk management

The output from this activity required by CII stakeholder organisations for their own risk management is:

- Guidelines (including soft rules) for self-regulation (O.1.5).

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A1: Set the Vision.

- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A1: Set the Vision.

A2: Establish NRM Organisation

Description

This activity takes into account political, market and security requirements in order to assign roles, responsibilities and tasks to appropriate key stakeholders within the NRM governance framework. It assigns appropriate tasks and co-ordinates actions within and between groups to ensure effective NRM synergies. It uses appropriate information flow and communication mechanisms to ensure stakeholders and key players are effective in complying with legal and regulatory requirements and fulfilling assigned roles.

Responsibilities

National governments have the responsibility for determining appropriate roles and responsibilities in relation to NRM; and, in conjunction with national security institutions, in assigning tasks, coordinating actions and carrying out national NRM exercises. National Security Institutions (see definition in footnote 1), in collaboration with sector regulators, have responsibility for helping to drive NRM standardisation, ensuring effective stakeholder collaboration and the development and use of appropriate communication and operating mechanisms. Individual organisations within the critical information infrastructure have responsibility for ensuring their involvement in the organisation of NRM.

Dependencies

This activity depends on the identification of appropriate stakeholders within activity A1.

Inputs to, and outputs from CII stakeholder risk management

Two outputs from this activity are required by CII stakeholder organisations for their own risk management:

- Information relating to co-ordinating actions (O.2.4);
- Standardisation of information (O.2.5).

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A2: Establish NRM Organisation.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A2: Establish NRM Organisation.

4.4. Description of Process 2: Coordinate and Support Implementation

This process contains all activities that are related to communication with, coordination of, and support for, the stakeholders identified and organised in the previous process. The process is intended to assist these organisations by making their own risk management processes more effective through monitoring these in the wider national context; and by providing information about emerging issues, awareness, coordination and the promotion of good practices.

A3: Support and Regulate

Description

This activity provides an appropriate support and regulation framework that is fully aligned with dynamic NRM policies, strategic goals and identified key stakeholders, taking into account political, market and security conditions, in order to provide appropriate regulation for NRM activities performed by those with identified roles and responsibilities. These activities ensure that NRM information is fully and effectively shared between them.

Responsibilities
National governments have the responsibility, in conjunction with national security institutions and sector regulators, for both providing an appropriate support and regulation framework and implementing effective information sharing schemes. Individual organisations within the critical information infrastructure have responsibility for ensuring their involvement in this support and information sharing framework.

Dependencies
This activity depends on the output of both activities A1 and A2.

Inputs to, and outputs from CII stakeholder risk management
The one output from this activity required by CII stakeholder organisations for their own risk management is:

- Information Sharing Schemes (O.3.2).

Measuring Strengths and Weaknesses
- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A3: Support and Regulate.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A3: Support and Regulate.

A4: Promote Awareness
This activity takes into account national policies and goals for awareness raising to develop effective material and programmes to train and educate clearly defined NRM participants and target groups. The effectiveness of the training material and programmes is monitored and measured and lessons are learned to ensure that continuous improvement takes place.

Responsibilities
Sector regulators, in conjunction with national security institutions, have responsibility for producing appropriate training and education material.

Dependencies
This activity depends on information about lessons learned as a result of the implementation of risk management in individual organisations.

Inputs to, and outputs from CII stakeholder risk management
The input to this activity required from CII stakeholder organisations' own risk management is:

- Lessons learned from implementation (I.20.5).

Measuring Strengths and Weaknesses
- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A4: Promote Awareness.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A4: Promote Awareness.

A5: Provide Necessary Information
This activity gathers timely, relevant and appropriate information on technical risks (threats, vulnerabilities, incidents and impacts) to information systems, and on the effectiveness of the mitigation and management of those risks, from identified stakeholder organisations. This information is aggregated and analysed in order to deliver statistical data on the national risk landscape and to share information to assist in the effective and timely coordination of future risk management actions.

Responsibilities

To ensure effective operation of the NRM governance framework, National Security Institutions (see definition in footnote 1) should ensure that they gather data on the national risk landscape and share that data appropriately.

Dependencies

This activity depends on information about risks (threat vulnerability and impact) drawn from risk management implementation in stakeholder organisations.

Inputs to, and outputs from CII stakeholder risk management

This activity requires a number of inputs from CII stakeholder organisations' own risk management:

- Outputs from A13 (see Annex B): (Define the scope of assessment: environment (internal, external) and assumptions (scope) of the assessment and risk criteria):
  - O.13.1 Identification method;
  - O.13.2 Likelihood data (e.g. history database);
  - O.13.3 Justification for threats and vulnerabilities intentionally disregarded;
  - O.13.4 Scope of risk assessment.
- Outputs from A14 (see Annex B): Identify Risk (Critical Assets /Services, vulnerabilities and threats (including inter-dependencies)):
  - O.14.1 List of relevant threats;
  - O.14.2 List of relevant vulnerabilities of (groups of) assets;
  - O.14.3 List of relevant impacts ;
  - O.14.4 List of values including frequency, severity and value of assets affected;
  - O.14.5 Interdependencies between sectors.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A5: Provide Necessary Information.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A5: Provide Necessary Information.

A6: Promote Standards

This activity gathers information on appropriate standards and best practices related to risk management preparedness. These are evaluated for their relevance and likely effectiveness in improving NRM methods. Existing NRM methods are adapted and updated accordingly. Key players in both public and private sectors are identified and information about new and improved standards and best practices and recommendations about adapted and updated methods are then disseminated to them. Checks are employed to ensure that they are used in a timely and effective manner.

Responsibilities

National security institutions and sector regulators have responsibility for gathering information on good practices and methods and for sharing that information appropriately.

Dependencies

This activity is not dependent on any other activity within this framework.

Inputs to, and outputs from CII stakeholder risk management

There are no implementation inputs to this activity from CII stakeholder organisations' risk management, or outputs from this activity to CII stakeholder organisations' risk management implementation.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A6: Promote Standards.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A6: Promote Standards.

A7: Foster Collaboration

This activity identifies intra- and inter-sectoral interdependencies between identified key players. It analyses and evaluates them to determine appropriate responses, including coordinated risk management and self-regulation where necessary. Responses are appropriately disseminated and national exercises are carried out to ensure the effective and efficient operation of inter- and intra-sectoral collaboration.

Responsibilities

National security institutions are responsible for ensuring the coordination of responses and determining soft rules for collaboration. National security institutions, in collaboration with sectoral regulators, are responsible for determining appropriate self-regulation regimes and for developing national NRM exercises. Individual stakeholder organisations have responsibility for cooperating with the collaborative and self-regulatory rules and for taking part in exercises as appropriate.

Dependencies

This activity is dependent on information sharing schemes from A3 and on individual organisation's risk management in relation to interdependencies and asset groups.

Inputs to, and outputs from CII stakeholder risk management

Inputs to this activity from CII stakeholder organisations' risk management are:

- Interdependencies between sectors (O.14.5);
- Qualified or quantified risks relative to each asset or asset group (O.15.6).

Outputs from this activity to CII stakeholder organisations' risk management are:

- Self regulation (O.7.2);
- Soft rules for collaboration (O.7.3).

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A7: Foster Collaboration.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A7: Foster Collaboration.

A8: Monitor Effectiveness

This activity monitors and gathers information about the occurrence of events related to NRM and their consequences for those stakeholders involved. Reports are collated and analysed in relation to clearly defined, agreed NRM performance indicators. The effectiveness of NRM is assessed in the light of performance and, where necessary and appropriate, timely proposals for the adaptation of NRM methods and activities are made.

Responsibilities

National government and security institutions, together with sector regulators are responsible for both consolidating performance indicators and making proposals for adaptation of NRM processes (see Annex A, Table 4).Table 1

Dependencies

This activity is dependent on individual organisation's risk indicators and reporting on security events.

Inputs to, and outputs from CII stakeholder risk management

Inputs to this activity from CII stakeholder organisations' risk management are:

- Reports on events and consequences to stakeholders (O.20.1);
- Internal indicators (O.20.3).

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A8: Monitor Effectiveness.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A8: Monitor Effectiveness.

4.5. Description of Process 3: Review, Reassess and Report

This process concerns the gathering, analysis and evaluation of feedback from risk management processes. Its function is to ensure that the NRM governance processes are continuously improved and updated.

A9: Analyse Errors and Incidents

Note: In order to aid communication with other parties, it is essential to define what is meant by 'incident' in relation to this activity. Any definition should include a description of potential impact. For example, a telecommunications incident could be defined as: "a loss of service affecting more than 500 lines (homes, businesses or individuals)" The definition should be undertaken by National Security Institutions (see definition in footnote 1), in discussion with appropriate CII operators.

This activity monitors and collects information about security errors and incidents from CERTs (and organisations with an equivalent function) within stakeholder organisations and from European and international cooperative schemes. Information about the efficiency and effectiveness of national incident and error handling and response is collated and analysed in the light of NRM performance indicators and adaptation and improvement proposals (from A8). Useful and timely risk assessments are carried out for nationally critical systems, on the basis of the reports and analysis. Collated reports and analysis concerning security error and incident handling are made and submitted to appropriate national authorities.

Responsibilities

National security institutions, together with sector regulators, are responsible for both producing individual risk assessments and submitting reports to national authorities.

Dependencies

This activity is dependent on the consolidated performance indicators and adaptation proposals from activity A8.

Inputs to, and outputs from CII stakeholder risk management

There are no implementation inputs to this activity from CII stakeholder organisations' risk management, or outputs from this activity to CII stakeholder organisations' risk management implementation. This because data on errors and incidents does not form an output from the risk management processes described in Annex B.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A9: Analyse Errors and Incidents.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A9: Analyse Errors and Incidents.

A10: Review Effectiveness

This activity determines evaluation criteria and quality parameters for the effectiveness of NRM processes and the NRM governance framework. It monitors information about NRM performance in response to incidents and issues. This is reviewed in the light of the performance criteria, evaluations based on organised survey data and on ongoing consultations with competent authorities. Audit reports are produced as a result of the review process and action plans based on the audit reports are documented and delivered.

Responsibilities

National governments and security institutions, together with sector regulators, are responsible for determining the effectiveness of NRM processes and the NRM governance framework. Sector regulators and national security institutions are responsible for delivering audit reports to competent authorities.

Dependencies

This activity is dependent on A1 and A8.

Inputs to, and outputs from CII stakeholder risk management

There are no implementation inputs to this activity from CII stakeholder organisations' risk management, or outputs from this activity to CII stakeholder organisations' risk management implementation.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A10: Review Effectiveness.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A10: Review Effectiveness.

A11: Report on NRM Process Maturity

This activity monitors the implementation of other NRM activities and gathers inputs including risk assessments for individual stakeholders, reports and analysis on security error and incident handling, reports on NRM process and the NRM framework effectiveness and NRM improvement action plans. This information is collated and analysed to evaluate current NRM performance. On the basis of this analysis, current NRM preparedness status reports are produced and disseminated.

Responsibilities

National security institutions are responsible for delivering national risk preparedness status reports to the competent authorities.

Dependencies

This activity is dependent on individual risk assessments and reports on errors and incidents from A9 and on NRM process and framework effectiveness reports and action plans from A10.

Inputs to, and outputs from CII stakeholder risk management

There are no implementation inputs to this activity from CII stakeholder organisations' risk management, or outputs from this activity to CII stakeholder organisations' risk management implementation.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A11: Report on NRM Process Maturity.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A11: Report on NRM Process Maturity.

A12: Suggest Improvements

This activity monitors and gathers NRM preparedness status reports. These are collated and analysed in relation to the overall picture of the critical information infrastructure (CII). On the basis of the analysis timely and effective action plans are produced to ensure the ongoing improvement of NRM preparedness and the NRM framework.

Responsibilities

National security institutions and sector regulators are responsible for delivering action plans for process and framework improvement to the competent authorities.

Dependencies

This activity is dependent on national risk preparedness status reports from A11.

Inputs to, and outputs from CII stakeholder risk management

There are no implementation inputs to this activity from CII stakeholder organisations' risk management, or outputs from this activity to CII stakeholder organisations' risk management implementation.

Measuring Strengths and Weaknesses

- Questions to assess the level of capability maturity in NRM preparedness for this activity can be found at: A12: Suggest Improvements.
- Questions to assess the level of capability maturity in CII stakeholder interaction for this activity can be found at: A12: Suggest Improvements.

5. Tools Associated with Framework for Governance of NRM

As part of its activities, the ENISA Working Group has developed a number of tools that may be used in connection with the framework for governance of NRM described in Section 4. These are as follows:

- Questionnaires for use by governments, national security agencies, CII sectoral regulators and CII stakeholder organisations to assess NRM capability maturity.
- A workflow for developing the framework for governance of NRM.
- A process for testing NRM preparedness.

Each of these three tools is described in the sections below.

5.1. NRM Capability Maturity Questionnaires

At Annex C is a questionnaire intended for use by either representatives of national governments or by representatives of regulatory bodies or of organisations that are major providers of critical information infrastructure. The purpose of this questionnaire is to give governments an assessment of their preparedness in the different activities of NRM; and thus the possible state of overall NRM preparedness in their country. The questionnaire is not intended to benchmark individual countries or to attempt comparisons between countries. The questionnaire is intended to be completed as a reflection of the opinion of the respondent.

A second version of the questionnaire, for use by representatives of CII stakeholder organisations, is shown in Annex D. The purpose of the data from this questionnaire is to assist governments in understanding the effectiveness of their NRM processes from the point-of-view of CII stakeholders. The questionnaire is intended to highlight those areas where coordination of, and communication with stakeholders could be further developed or improved. It is not intended to benchmark individual countries or to attempt comparisons between countries. The questionnaire is intended to reflect the awareness of the respondent concerning their government's NRM activities.

A spreadsheet has also been produced, and will be made available to accompany this report. The spreadsheet will enable organisations to capture questionnaire data, analyse the results and create graphical reports; also to aggregate individual country data and compare data from up to 10 countries. The method of using the spreadsheet is fully explained in Annex E.

5.2. NRM Development Workflow

In seeking to improve their NRM, governments may find it useful to follow a clear developmental path. Figure 5, below, shows a flow diagram that illustrates such a path; the five main elements of which (as indicated by the coloured boxes) are as follows:

- Assess strengths and weaknesses;
- Develop process P1;
- Develop process P2 and;
- Develop process P3
- Test NRM preparedness (described in Section 5.3).

The actions shown in this workflow are described, step-by-step, below. It should be noted that in Figure 5 the 12 activities (A1 to A12) have been broken down into individual actions (e.g.: A1.1, A1.2), where appropriate. Figure 5 shows the method by which the NRM processes may be developed; for information about the flow of collaborative activity between governments and stakeholders, see Annex A and Annex B.

The workflow begins with the use of the questionnaires (as discussed in Section 5.1) to assess strengths and weaknesses in the current NRM. As Figure 5 indicates, if use of the questionnaire

assesses that NRM policy definition (process P1) does not have an appropriate level of capability maturity, governments should first ensure that they have set clear strategic objectives, as well as the policies to support these. Appropriate stakeholders should then be identified and data relating to these should be documented. Roles and responsibilities should be assigned to relevant stakeholders in accordance with national security requirements and market conditions. The most critical activity in P1 is to ensure that the functions of stakeholders, with assigned roles and responsibilities, are coordinated and that their actions are compliant with policy requirements.

Once it has been assessed that process P1 has been implemented to an appropriate level of capability maturity, governments need to consider coordination and support of risk management implementation in CII stakeholder organisations, within the national context (process P2). As Figure 5 shows, this first involves setting up an effective support and regulation framework for those stakeholders given roles and responsibilities under process P1. This should lead to successful information sharing; an essential activity that flows from stakeholder coordination, as established in process P1. Information, however, can only be effectively acted on if stakeholders are given the appropriate education, training and awareness – the next activity in the implementation process. Coordination and compliance by stakeholders (process P1) will also ensure that relevant and timely information about risk management in their organisations is passed to appropriate government agencies. This, together with information about best practices and methodologies, should be analysed and shared appropriately. Finally, the implementation process should ensure that interdependencies between stakeholders are understood so that effective collaborative responses can be tested and appropriate lessons learned.

Preliminary indications (see Section 6) are that the review and improvement process for NRM (P3) may be the least highly developed in EU member states. Governments should therefore consider devoting increased resources to the activities that constitute this process, including: performing national risk assessments in the light of incidents; collating and reviewing incident reports in the light of established evaluation criteria and; issuing audit reports and action plans on the basis of the review and analysis. Finally, assessments should be made to consider what improvements, if any, are needed – and improvement plans should be established and implemented where necessary. Please note that activities within P3 include the reassessment and update of the framework for governance of NRM, where appropriate and necessary.

Organisations will also wish to use the inputs and outputs to and from the framework for governance of NRM, as shown in Table 4 (Annex B), as a checklist to ensure that all the elements required by an activity are present. For example, in assessing their ability to set the vision for NRM (activity A1), they will wish to ensure that they are able to take advantage of the following inputs:

- Relevant political, ministerial and EU parliamentary decisions.
- Relevant national laws and EU directives.
- Reports on national risk preparedness status (an output from action A10).
- Action plans for NRM framework and process improvement (an output from action A12).

If all processes and activities are deemed to be satisfactorily established and implemented, governments will find it appropriate to test their NRM preparedness (indicated by the box labelled “Test NRM Preparedness” at the top of Figure 5). This will ensure that the national risk management is functioning effectively and according to requirements. The next section (Section 5.3) defines a test process for NRM preparedness.

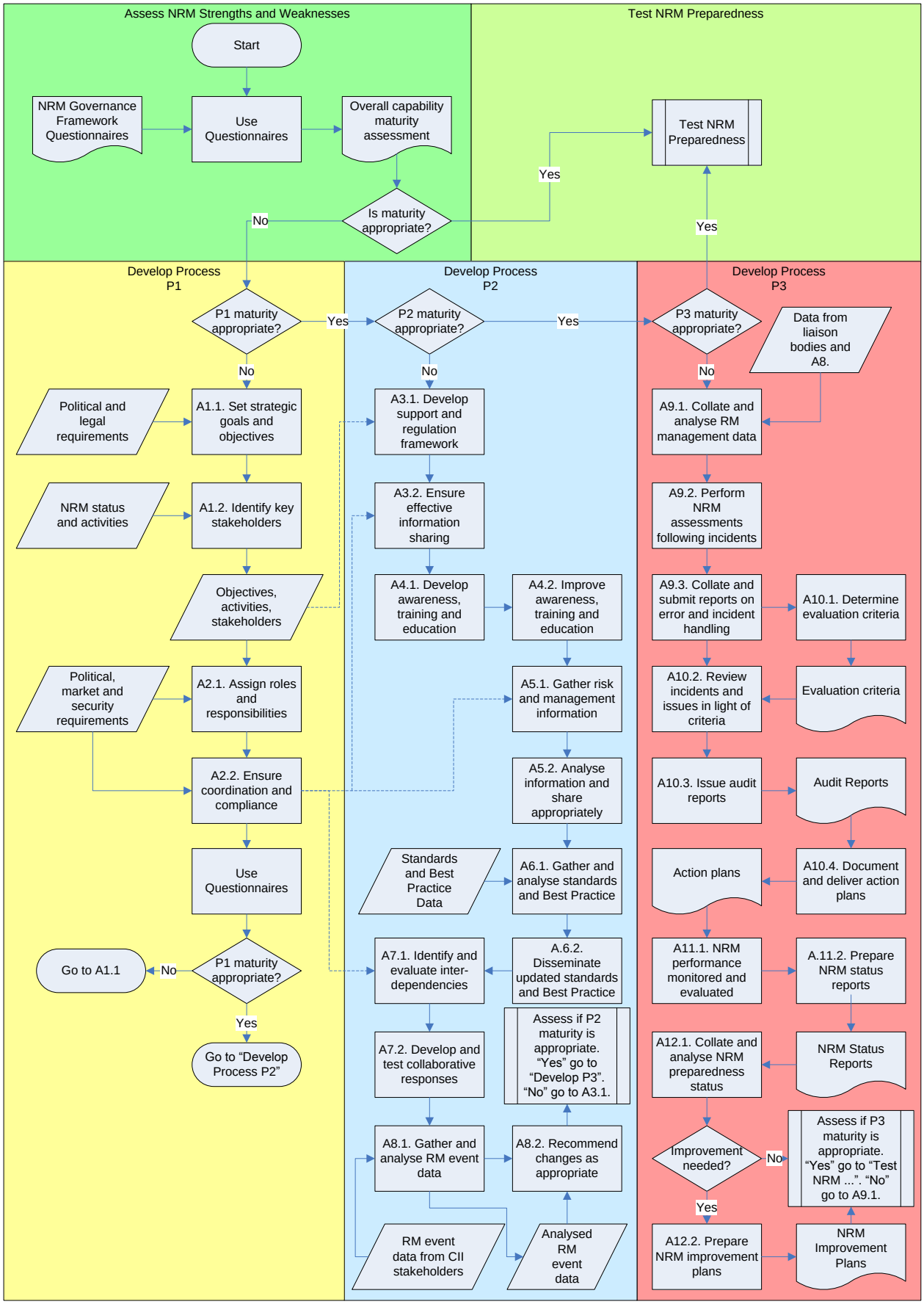

Figure 5: Flow Diagram for the Development of a NRM Governance Framework

5.3. Testing NRM Preparedness

In order to test the preparedness of EU member states' NRM, it is suggested that a simple, generic test process is followed. This is illustrated in Figure 6, below.

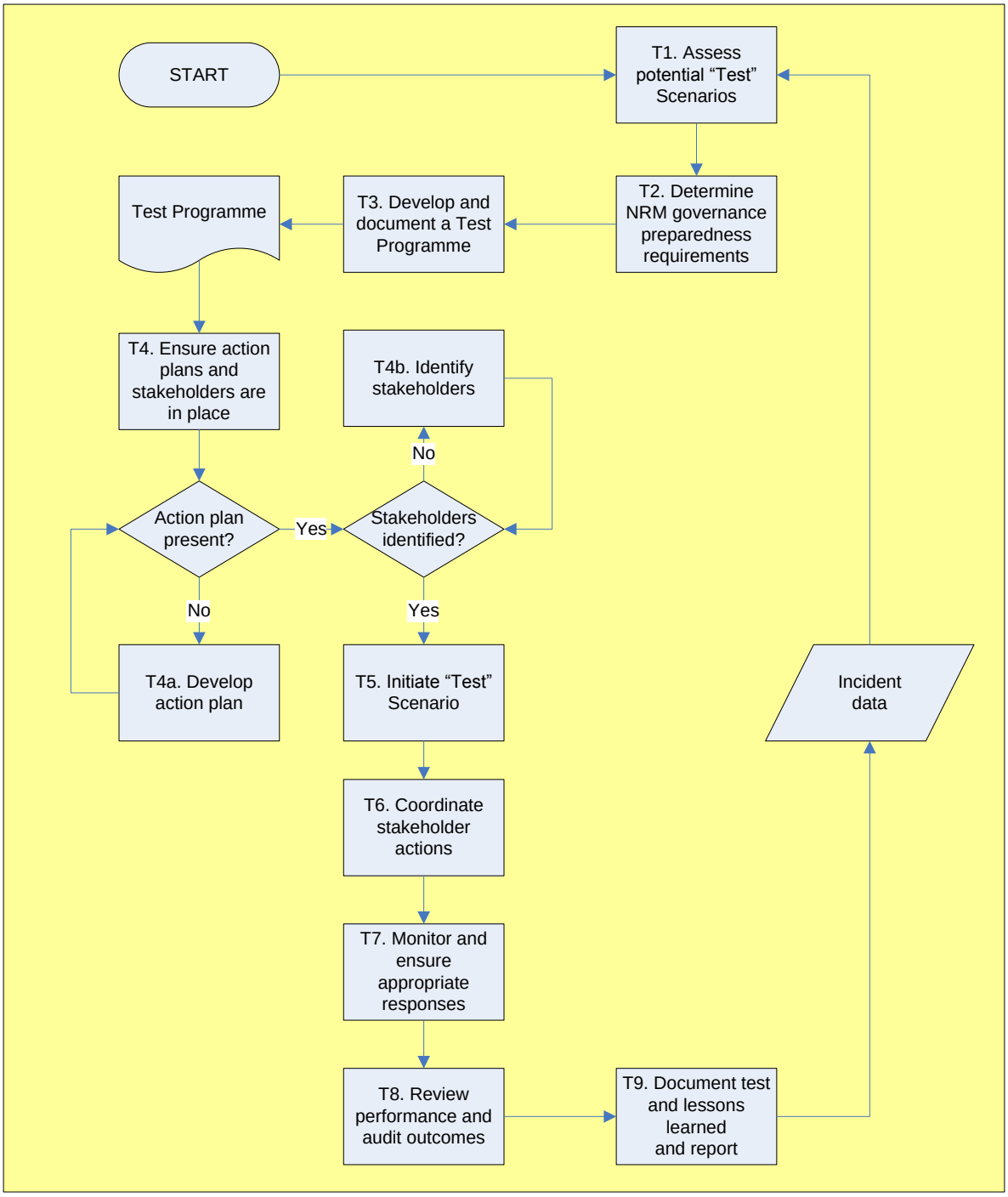

Figure 6: NRM Governance Framework Testing - Flow Diagram

As Figure 6 shows, the NRM preparedness test process consists of 9 activities, labelled T1 to T9 in the figure. Each of these activities is considered briefly in the sections below.

T1. Assess Potential "Test Scenarios"

In Figure 6, the recommended course of action is to begin by assessing appropriate potential test "scenarios". These could be assessed from records of incidents which have actually occurred –

perhaps in other EU member states. Alternatively, potential scenarios could be assessed from incidents which could be predicted to occur; given technological changes or known vulnerabilities[5].

Areas that could be used as subjects of test scenarios might be all those which have the potential to impact on the resilience of public electronic networks. These include:

- Potential for hostile attack on government networks.
- Potential for hostile attack on financial networks.
- Potential for hostile attack on SCADA interfaces with the internet, as used by major utilities.
- Potential for major loss of telecommunications or ISP functionality as a result of natural disaster or serious human error.
- Potential loss of significant government applications as a result of technology issues or serious human error.

When selecting a scenario, governments should consider the incident data resulting from any previous NRM preparedness tests. This will help to ensure that scenarios are selected which examine the "lessons learned". In particular, scenarios should be selected which are likely to test those NRM activities where there was previously poor coordination or compliance by stakeholders.

T2: Determine NRM Governance Preparedness Requirements

In this activity, governments should consider the level of capability maturity at which they need to test their NRM preparedness. If the risk posed by the scenario is somewhat lower, or the national state of preparedness is such that a less rigorous standard of preparedness is acceptable; governments may wish to test to a medium, rather than a high level of capability maturity. Please note that it is not recommended that NRM preparedness be subject to test if the capability maturity of the overall NRM governance framework has been assessed as "low".

Table 2, below, shows which of the NRM activities are subject to test and which inputs and outputs might be expected at both medium capability maturity (level 3-4) and high capability maturity (level 4-5).

NRM Preparedness Capability Maturity	NRM Activity	Inputs to Activity	Outputs from Activity
MEDIUM (Level 3-4)	A1: Set the vision	Relevant national political decisions.	Goals and objectives. Incentives for collaboration. Competent authorities.
	A2: Establish NRM organisation	Security incident data. Identified key players and roles. Regulations.	Task assignment. Coordinating actions. Public/private collaborations. Role assignment. Determined information flows. Communications mechanisms and their use.

[5] Scenarios of this type have been the subject of the ENISA work programme on emerging and future risks: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk

NRM Preparedness Capability Maturity	NRM Activity	Inputs to Activity	Outputs from Activity
	A3. Support and regulate	Goals and objectives. Incentives for collaboration. Competent authorities. Task assignment. Coordinating actions. Public/private collaborations. Role assignment. Determined information flows. Communications mechanisms and their use.	Support and regulation framework. Information sharing scheme.
	A5. Provide necessary information	Information from CERTs. Identified stakeholders. List of relevant threats, vulnerabilities, impacts and impact values. Interdependencies between sectors.	Shared information.
	A7. Foster collaboration	Identified main players. Identified coordination mechanism. Information sharing scheme. Interdependencies between sectors. Quantified risk in relation to asset groups.	Coordinated response. Soft rules for collaboration.
	A8. Monitor effectiveness	Reports on events and consequences. Internal indicators.	Consolidated performance indicators.
	A9. Analyse errors and incidents	Errors, incidents and criticality. CERT information. Consolidated performance indicators.	Communication to competent authorities.
	A10. Review effectiveness	Errors, incidents and criticality. Communication to competent authorities. Consolidated performance indicators.	Identified NRM framework and process effectiveness. Action plans to improve effectiveness.
HIGH (Level 4-5)	A1. Set the vision	Political decisions. Laws. Ministerial decisions. European directives. EU parliament decisions. National risk preparedness status reporting. Action plans for NRM framework and process improvement.	National regulation. Goals and Objectives. Incentives for collaboration. Competent authorities. Self regulation, Soft rules for regulation.

NRM Preparedness Capability Maturity	NRM Activity	Inputs to Activity	Outputs from Activity
	A2: Establish NRM organisation	Political priorities. Market needs. Security incidents. National security issues. Political consultation meetings. Identified key players and their role. Regulation.	Roles and responsibilities to authorities. Task assignment. Coordination actions. Standardisation. Public, private collaborations. Role assignment within national exercises. Determination of information flows among stakeholders. Communication mechanisms. Use of the communication mechanisms.
	A3. Support and regulate	National regulation. Goals and Objectives. Incentives for collaboration. Competent authorities. Self regulation, Soft rules. Roles and responsibilities to authorities. Task assignment. Coordination actions. Standardisation. Public, private collaborations. Determination of information flows among stakeholders. Communication mechanisms and their use.	Support and regulation framework. Information Sharing schemes.
	A5. Provide necessary information	Information provided by CERTs. Identified stakeholders. Identification method. Likelihood data. Justification for threats and vulnerabilities intentionally disregarded. Scope of risk assessment. List of relevant threats. List of relevant vulnerabilities of asset groups. List of relevant impacts. List of values including frequency, severity and value of assets affected. Interdependencies between sectors.	Statistical data on national risk landscape. Data on national risk landscape. Shared information.

NRM Preparedness Capability Maturity	NRM Activity	Inputs to Activity	Outputs from Activity
	A7. Foster collaboration	Identified main players and sectors in terms of criticality. Identified mechanism and the coordinating model. Information Sharing schemes. Interdependencies between sectors. Qualified or quantified risks relative to each asset or asset group.	Coordinated response. Self regulation. Soft rules for collaboration.
	A8. Monitor effectiveness	Reports on events and consequences to stakeholders. Internal indicators.	Consolidated performance indicators. Adaptation proposals.
	A9. Analyse errors and incidents	Errors and incidents. Identified levels of criticality of incidents. European / International cooperation schemes. CERT information. Consolidated performance indicators. Adaptation proposals.	Requirements for individual risk assessments. Communication to competent authorities.
	A10. Review effectiveness	Errors and incidents. Communication to competent authorities. Performance indicators.	Identified NRM framework and process effectiveness. Action plans to improve effectiveness.
	A11. Report on NRM process maturity	Requirements for individual risk assessments. Communication to competent authorities. Identified NRM framework and process effectiveness. Action plans.	National risk preparedness status reporting.
	A12. Suggest improvements	National risk preparedness status reporting.	Action plans for NRM framework and process improvement.

Table 2: NRM Activities, Inputs and Outputs Expected at Medium and High Capability Maturity

T3. Develop and Document a Test Programme

Once a potential scenario has been selected and the NRM preparedness requirements have been determined, a test programme should be developed and documented. The document should describe programme elements such as:

- Essential pre-conditions for the test.
- Who will carry out different aspects of the test. Please note that high level responsibilities and dependencies for each of the activities have been identified in sections 4.3, 4.4 and 4.5, and in Annex A and Annex B.
- How the test will be initiated.
- The sequence of activities expected to follow test initiation.
- The expected outcomes and deliverables from the test.
- Service level objectives and performance metrics for the test.

T4. Ensure Action Plans and Stakeholders are in Place

Using the test programme document, a paper exercise should be conducted to ensure that appropriate action plans and stakeholders are in place to deal with the test programme. Where an appropriate action plan does not exist, this should be developed, or an existing plan should be modified (activity T4a. in Figure 6). The stakeholders needed by the test programme should also be identified and notified, if this has not already been done (action T4b. in Figure 6).

T5. and T6. Initiate and Coordinate

Once all the pre-conditions are in place, the test should be initiated as specified in the test programme document. The group or agency responsible for overseeing the test should ensure that the actions of all the identified stakeholders are properly coordinated and take place in the sequence specified.

T7. and T8. Monitor and Review

The agency or group responsible for monitoring and performance review should check that expected outcomes and deliverables are in accordance with service level objectives and performance metrics specified in the test programme document. Finally, the results of the test should be collated by the group responsible for reviewing test outcomes and auditing NRM test performance.

It should be noted that, while many of these roles may be shared by one or two groups, it is not recommended that the same individuals take responsibility both for overseeing or carrying out the tests and for monitoring, reviewing or auditing performance and outcomes. This separation will help to ensure objectivity and lack of bias in the assessment of the test.

T9. Document Test and Lessons Learned and Report

The report on the test, its performance and outcomes, should be fully documented and the report presented to the appropriate authorities. Where necessary, failures in the testing programme should be identified and lessons learned should be highlighted. Recommendations for improving processes and activities within the framework for governance of NRM should be made where necessary. The data on the test should be stored so that it can be retrieved and used in the selection and planning of future test programmes.

6. Report on NRM Preparedness in EU Member States

The Working Group undertook the first step in the development process ("Assess NRM strengths and weaknesses", described in Section 5.2), by using the questionnaire (see Section 5.1), to ask respondents from four EU member states[6] to assess the current capability maturity of their governments in relation to NRM. As a result of this activity, the Working Group was able achieve its main goal, namely to test the applicability of the framework for governance of NRM; and as a secondary goal and to draw some preliminary conclusions concerning NRM preparedness in those EU member states surveyed. It is worth mentioning, that the small sample of the first assessment has indicative value and should NOT be considered as being representative for other/many EU Member States.

The data obtained through use of the questionnaires was normalised and analysed. Table 3 below, shows the results of the normalisation and analysis, indicating respondents' assessment of capability maturity (using the COBIT capability maturity measurement scale of 1 to 5) in each of the 12 NRM activities (A1 to A12), for each of the four countries studied. The average assessment for each of the 3 processes and 12 activities and for each of the countries is also given.

Process	Activity	Countries				Averages	
		A	B	C	D	Process	Activity
P1.	A1. Set the vision	3.83	1.83	2.5	4.50	**3.12**	**3.17**
	A2. Establish NRM organisation	2.83	2.50	2.5	4.50		**3.08**
P2.	A3. Support and regulate	2.50	2.50	2.5	4.00	**2.82**	**2.88**
	A4. Promote awareness	2.83	2.00	3.5	3.00		**2.83**
	A5. Provide necessary information	2.67	2.00	2.5	5.00		**3.04**
	A6. Promote standards	1.33	2.83	3	5.00		**3.04**
	A7. Foster collaboration	2.17	2.00	2.5	5.00		**2.92**
	A8. Monitor effectiveness	1.33	2.00	2.5	3.00		**2.21**
P3.	A9. Analyse errors and incidents	2.33	2.67	2.5	3.50	**2.44**	**2.75**
	A10. Review effectiveness	1.67	2.00	2	4.00		**2.42**
	A11. Report on NRM process maturity	1.33	2.00	1.5	4.50		**2.33**
	A12. Suggest improvements	1.50	2.00	1.5	4.00		**2.25**
Country Averages		**2.19**	**2.19**	**2.42**	**4.17**		

Table 3: NRM Preparedness Estimates for Four EU Countries

It is evident that, with such a small sample size, very little can be deduced about the state of NRM preparedness within the EU as a whole. Furthermore, it is important to be clear that the purpose of using the questionnaires was not to "benchmark" NRM preparedness in EU countries, but to test the operation of the questionnaire and the applicability of the framework for NRM governance. For this reason, the individual countries are not identified in Table 3.

However, it seems clear from the results obtained, that P1 (Define NRM Policy) is more mature than P2 (Coordinate and Support Implementation), while that process is in turn is more mature than P3

[6] Two small member states, one medium and one large.

(Review, Reassess and Report). Overall, the least mature activity appears to be A8 (Monitor effectiveness). Although the results are only preliminary and indicative it would seem that there may be wide variation between EU member states in their NRM preparedness. However, it is possible to conclude that all those surveyed assess themselves as being less mature in the review and updating of their governance of NRM than they are in policy setting and promoting awareness.

Wider use of the questionnaire could enable EU member states to identify more confidently those areas where improvement is generally required. This could in turn enable EU member states to offer more targeted guidance and assistance to individual CII stakeholders. Further work could also be usefully done, using the CII stakeholder questionnaire, in order to determine the effectiveness of national governments in promoting risk management throughout their CII communities.

7. Open Issues and Further Work

The activities of the Working Group on NRM preparedness, as described in this document, have formed the basis for understanding both how EU member states can develop a standardised framework for the governance of their NRM and how they can test their NRM preparedness. However, some issues have not been fully dealt with by this work and further effort may usefully be carried out in a number of areas. Among these are the following:

1. Resolving issues concerning the confidentiality of NRM activities and the degree to which information relating to these activities can be shared with, and between, CII stakeholder organisations.
2. Developing processes for consolidating different NRM governance capability maturity levels in different sectors. For example, the implications for overall NRM preparedness where different sectors have very different levels of capability maturity in their implementation of risk management.
3. The possibility of generalising the framework for NRM governance to enable its use in risk management governance within individual organisations; particularly those with disparate physical or logical constituent groups.
4. The definition of Key Performance Indicators (KPIs) for all activities involved in order to better (more objectively) identify maturity levels; but also to offer better support to interested parties in the governance of risk management.
5. Wider use of the questionnaires within EU member states to determine strengths and weaknesses of NRM governance throughout the EU.
6. The possibility of implementing a programme of test scenarios in EU member states to investigate NRM preparedness more widely.

The above mentioned open issues can be addressed via a variety of ways. ENISA, in cooperation with experts from Member States could take care of the points 1-4. Such an activity could be part of work on Security Governance or could be performed by means of a Working Group. Points 5 and 6, in turn, could be performed under coordination of the Commission together with the Member States with the support of ENISA.

8. Bibliography

The following works are referenced within this document:

- Who-is-Who. Directory on Network and Information Security. Edition 2010. ENISA.
- Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. European Commission communication 2009 (COM (2009) 149).
- A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet. European Commission research report commissioned 2008 (JLS/2008/D1/018).
- ISO/IEC 27005: 2008 (Information security – Security techniques – Information security risk management).
- ISO/IEC 27001: 2005 (Information security – Security techniques – Information security management systems – Requirements).
- Methodology for evaluating usage and comparison of risk assessment and risk management items. Deliverable 2 of the ENISA WG 2 on Risk Assessment and Management, published 26th April 2007.
- COBIT 4.1. ISBN 1-933284-72-2. Copyright IT Governance Institute 2007.
- "Security and Resilience in Governmental Clouds"(published January 17th 2011) and "Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology" (published April 12th 2010). Reports by ENISA Working Groups on Emerging and Future Risks.

Annex A: Framework for NRM Governance – Inputs and Outputs

Figure 7, below, shows the process-flow relationship between the inputs and outputs of the 12 activities of the framework for NRM governance described in Section 4. The inputs and outputs are colour-coded (see the Key) to indicate which inputs are derived from the framework for risk management in individual organisations (pink) and which outputs go to the framework for risk management in individual organisations (yellow). Outputs from the 12 NRM governance activities, which form inputs to other activities within this framework, are coloured blue/grey. The arrows indicate where outputs from one activity act as inputs to another activity within this framework.

Table 4, which follows the figure, gives an explanation of the input and output numbering, and also summarises the responsibilities for inputs and outputs. The abbreviations for responsibilities are labelled as in Table 1.

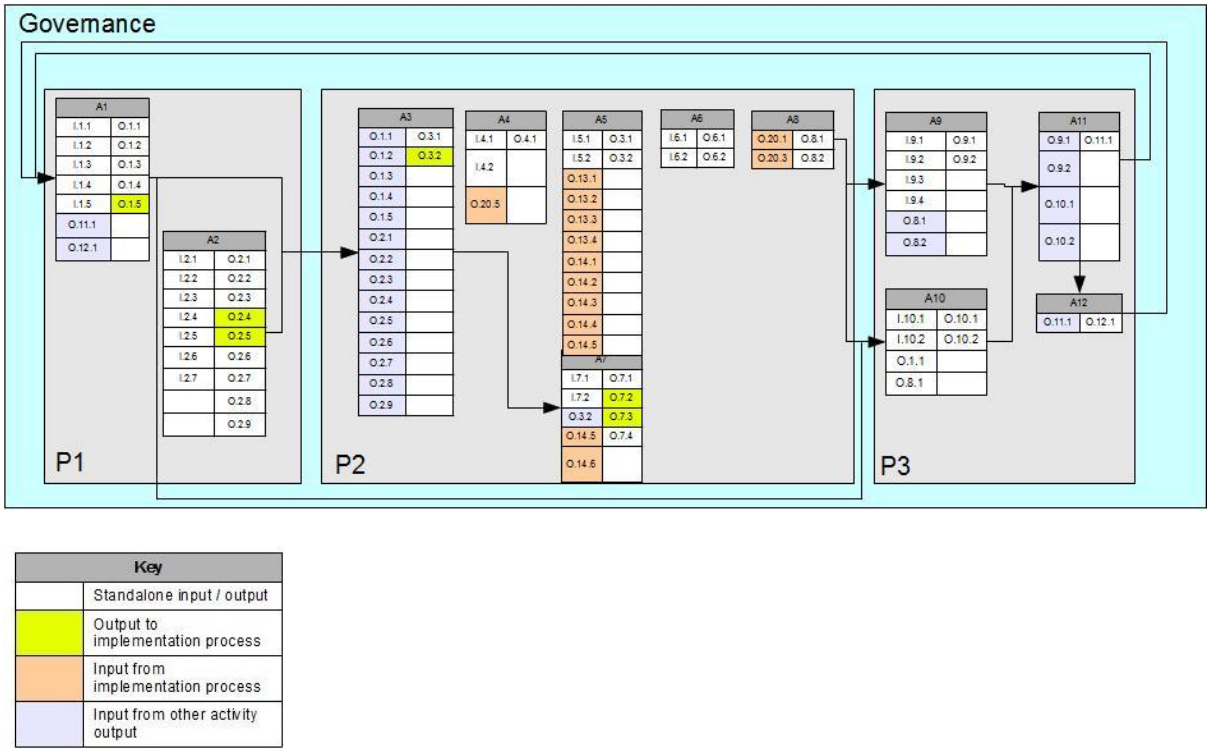

Figure 7: Inputs and outputs to and from the NRM Governance Framework

Note: The naming and description of inputs and outputs in the table below is indicative only and may be varied in accordance with the circumstances and requirements of the users of the framework.

Process	Activity	Input	Output
Process 1: Define NRM Policy	A1. Set the vision	**I.1.1** Political decisions (NG) **I.1.2** Laws (NG) **I.1.3** Ministerial decisions (NG) **I.1.4** European directives (NG) **I.1.5** EU parliament decisions (NG) **O.11.1** National risk preparedness status reporting (NSI) **O.12.1** Action plans for NRM framework and process	**O.1.1** National regulation (NG, SR) **O.1.2** Goals and Objectives (NG) **O.1.3** Incentives for collaboration (NG) **O.1.4** Competent authorities (NG) **O.1.5** Self regulation, Soft rules for regulation (SR, NSI, IO)

Process	Activity	Input	Output
		improvement (SR, NSI)	
	A2. Establish NRM organisation	**I.2.1** Political priorities (NG) **I.2.2** Market needs (IO) **I.2.3** Security incidents (NG, SR, NSI) **I.2.4** National security issues (NSI) **I.2.5** Political consultation meetings (NG) **I.2.6** Identified key players and their role (SR, NSI) **I.2.7** Regulation (SR, NSI)	**O.2.1** Roles and responsibilities to authorities (NG) **O.2.2** Task assignment (NG, NSI) **O.2.3** Coordination actions (NG, NSI) **O.2.4** Standardisation (SR, IO, NSI) **O.2.5** Public, private collaborations (SR, IO, NSI) **O.2.6** Role assignment within national exercises (NG, NSI) **O.2.7** Determination of information flows among stakeholders (e.g. hierarchy, priorities, confidentiality arrangements) (SR, NSI) **O.2.8** Communication mechanisms (SR, NSI) **O.2.9** Use of the communication mechanisms (SR, NSI)
Process 2: Coordinate and Support Implementation	A3. Support and regulate	***Output from A1 and A2*** **O.1.1** National regulation (NG, SR) **O.1.2** Goals and Objectives (NG) **O.1.3** Incentives for collaboration (NG) **O.1.4** Competent authorities (NG) **O.1.5** Self regulation, Soft rules (SR, NSI, IO) **O.2.1** Roles and responsibilities to authorities (NG) **O.2.2** Task assignment (NG, NSI) **O.2.3** Coordination actions (NG, NSI) **O.2.4** Standardisation (SR, IO, NSI) **O.2.5** Public, private collaborations (SR, IO, NSI) **O.2.6** Role assignment within national exercises (NG, NSI) **O.2.7** Determination of information flows among stakeholders (e.g. hierarchy, priorities, confidentiality arrangements) (SR, NSI) **O.2.8** Communication mechanisms (SR, NSI) **O.2.9** Use of the communication mechanisms (SR, NSI)	**O.3.1** Support and regulation framework (NG, SR, NSI) **O.3.2** Information Sharing schemes (NG, SR, NSI, IO)
	A4. Promote awareness	**I.4.1** Goals of the raising actions (NG, SR, NSI) **I.4.2** Defined participants and target groups (SR, NSI)	**O.4.1** Education and training material (SR, NSI)

Process	Activity	Input	Output
		O.20.5 Lessons learned from implementation.	
	A5. Provide necessary information	**I.5.1** Information provided by CERTs (NSI) **I.5.2** Identified stakeholders (SR, NSI) *Output from A13* **O.13.1** Identification method **O.13.2** Likelihood data (e.g. history database) **O.13.3** Justification for threats and vulnerabilities intentionally disregarded **O.13.4** Scope of risk assessment *Outputs from A14* **O.14.1** List of relevant threats **O.14.2** List of relevant vulnerabilities of (groups of) assets **O.14.3** List of relevant impacts **O.14.4** List of values including frequency, severity and value of assets affected **O.14.5** Interdependencies between sectors	**O.5.1** Statistical data on national risk landscape (NSI) **O.5.2** Data on national risk landscape (NSI) **O.5.3** Shared information (NSI)
	A6. Promote standards	**I.6.1** Identified mechanisms to create/evaluate good practices and standards (SR, NSI) **I.6.2** Specified target groups (SR, NSI)	**O.6.1** List of good practices for dissemination (to stakeholders) (SR, NSI) **O.6.2** Proposal for methods to be used (SR, NSI)
	A7. Foster collaboration	**I.7.1** Identified main players and sectors in terms of criticality (SR, NSI) **I.7.2** Identified mechanism and the coordinating model (SR, NSI) **O.3.2** Information Sharing schemes (from A3) **O.14.5** Interdependencies between sectors (NSI) **O.15.6** Qualified or quantified risks relative to each asset or asset group (NSI)	**O.7.1** Coordinated response (NSI) **O.7.2** Self regulation (SR, IO, NSI) **O.7.3** Soft rules for collaboration (NSI, IO) **O.7.4** Plans for national exercises (NSI,S/ R, M)
	A8. Monitor effectiveness	**O.20.1** Reports on events and consequences to stakeholders (SR, NSI) **O.20.3** Internal indicators	**O.8.1** Consolidated performance indicators (NG, SR, NSI) **O.8.2** Adaptation proposals (NG, SR, NSI)
Process 3: Review, Reassess and Report	A9. Analyse errors and incidents	**I.9.1** Errors and incidents (NSI) **I.9.2** Identified levels of criticality of incidents (NSI) **I.9.3** European / International cooperation schemes (SR, NSI)	**O.9.1** Requirements for individual risk assessments (SR, NSI) **O.9.2** Communication to competent authorities (SR, NSI)

Process	Activity	Input	Output
		I.9.4 CERT information (NSI) **O.8.1** Consolidated performance indicators (output from A8) **O.8.2** Adaptation proposals (output from A8)	
	A10. Review effectiveness	**I.10.1** Errors and incidents (NSI) **I.10.2** Communication to competent authorities (SR, NSI) **O.1.1** Goals and objectives **O.8.1** Consolidated performance indicators (NSI)	**O.10.1** Identified NRM framework and process effectiveness (NG, SR, NSI) **O.10.2** Action plans to improve effectiveness (R,I)
	A11. Report on NRM process maturity	*Outputs from NRM process review (NSI)* **O.9.1** Requirements for individual risk assessments (SR, NSI) **O.9.2** Communication to competent authorities (SR, NSI) **O.10.1** Identified NRM framework and process effectiveness (NG, SR, NSI) **O.10.2** Action plans (R,I)	**O.11.1** National risk preparedness status reporting (NSI)
	A12. Suggest improvements	*Output of A11* **O.11.1** National risk preparedness status reporting (NSI)	**O.12.1** Action plans for NRM framework and process improvement (SR, NSI)

Table 4: Inputs, outputs and responsibilities for the NRM Governance Framework

Annex B: ENISA Risk Management Implementation Framework for Individual Organisations

Figure 8 below shows the relationship between the inputs and outputs of the 6 processes (P4-P9) and 8 activity groups (A13-A20) used for risk management implementation, as defined by the ENISA Working Group on Risk Assessment and Management. The inputs and outputs are colour-coded (see the Key) to indicate which inputs are derived from the framework for NRM governance (yellow) and which outputs go to the framework for NRM governance (pink). Outputs from the activities which form inputs to other activities within this framework are coloured blue/grey. The arrows indicate where outputs from one activity act as inputs to another activity within this framework. This figure is followed by Table 5. This lists these inputs and outputs, with their numbering, as well as showing responsibilities for them (labelled as in Table 1).

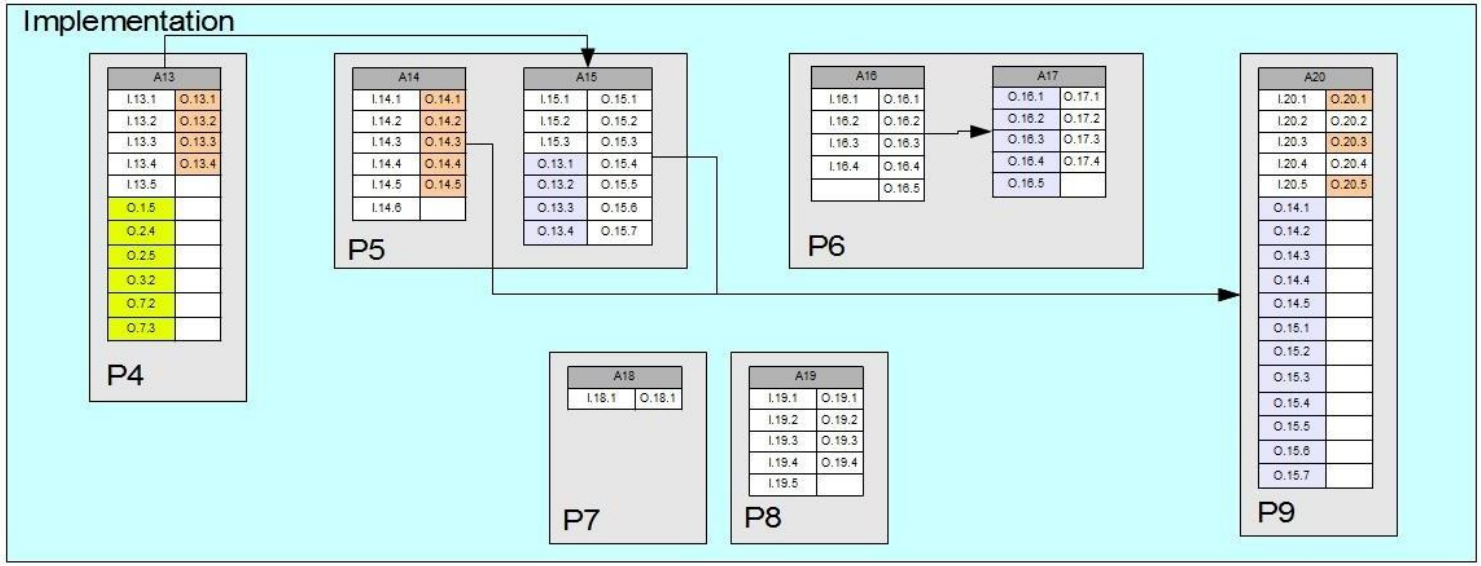

Figure 8: Processes, inputs, outputs and flows for risk management implementation framework

Note: The naming and description of inputs and outputs in the table below is indicative only and may be varied in accordance with the circumstances and requirements of the users of the framework.

Process	Activity	Description	Inputs	Outputs
Process 4: Definition of scope	**A13** Define the scope of assessment: environment (internal, external) and assumptions (scope) of the assessment and risk criteria	Identification of the method to be used for the risk assessment. Creation of a likelihood data repository and justification of vulnerabilities to be disregarded.	**I.13.1** Determined methodology to be used for the identification of risks (i.e. threats, vulnerabilities and impacts) (NSI, SR) **I.13.2** Threats, vulnerabilities and impact statements that will be used in the assessment (NSI, SR) **I.13.3** Checklists and tools for the assessment (NSI, SR) **I.13.4** Strategy on the organization (goals, objectives, etc.) **I.13.5** Assets in terms of resources (People, systems, processes, etc.) **O.1.5** Self regulation, Soft rules for regulation (SR, NSI, IO) **O.2.4** Standardisation (SR, IO, NSI) **O.2.5** Public, private collaborations (SR, IO, NSI) **O.3.2** Information Sharing schemes (NG, SR, NSI, IO) **O.7.2** Self regulation (SR, IO, NSI) **O.7.3** Soft rules for collaboration (NSI, IO)	**O.13.1** Identification method **O.13.2** Likelihood data (e.g. history database) **O.13.3** Justification for threats and vulnerabilities intentionally disregarded **O.13.4** Scope of risk assessment
Process 5: Risk Assessment	**A14** Identify Risk (Critical Assets /Services, vulnerabilities and threats (including inter-dependencies))	Identification of lists regarding threats, vulnerabilities, impacts and values as well as definition of interdependencies between sectors based on data from national risk landscape.	**I.14.1** Statistical data on national risk landscape (NSI, SR) **I.14.2** Data on national risk landscape (NSI, SR) **I.14.3** Historical information that can be used to assess the likelihood of impact (NSI, SR) **I.14.4** Scope of risk assessment **I.14.5** Description of the main business processes **I.14.6** Description of internal assets	**O.14.1** List of relevant threats **O.14.2** List of relevant vulnerabilities of (groups of) assets **O.14.3** List of relevant impacts **O.14.4** List of values including frequency, severity and value of assets affected **O.14.5** Interdependencies between sectors

Process	Activity	Description	Inputs	Outputs
	A15 Analyse and evaluate/prioritise the risks	Asset classification according to the classification scheme and creation of lists associating threats and vulnerabilities to assets. Formal decisions about the types of risks that should be treated.	**I.15.1** List of relevant threats with information about risk limits and classification scheme for assets **I.15.2** List of existing controls (technical/organisational) *Output of A13* **O.13.1** Identification method **O.13.2** Likelihood data (e.g. history database) **O.13.3** Justification for threats and vulnerabilities intentionally disregarded **O.13.4** Scope of risk assessment	**O.15.1** Tables with assets classified according to the classification scheme **O.15.2** List of threats and vulnerabilities relative to each asset **O.15.3** List of existing controls relative to each asset (part of so-called gap analysis) **O.15.4** List of impacts relative to each asset **O.15.5** List of risks relative to each asset **O.15.6** Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group) **O.15.7** Formal decision about previously analysed risks and about which risks will be treated (and possibly with what priority) or left untreated
Process 6: Risk Treatment	**A16** Identify and select treatment risk options, approve implementation, agree performance metrics and assign resources	Identification and selection of risk options based on defined criteria. Assignment of resources and responsibilities and creation of approved lists with activities.	**I.16.1** List with criteria for the forthcoming assessment activities **I.16.2** Assigned organisational roles **I.16.3** Possible planning methodology **I.16.4** Possible priority scheme to be used	**O.16.1** Risk treatment options according to risks (possibly classified according to the risk limits) **O.16.2** Action plan as sequence of prioritized activities (expressed as implementation of controls or as protection of assets) **O.16.3** Assignment of resources (e.g. costs) for action plan implementation **O.16.4** Assignment of responsibilities for each action **O.16.5** Approved lists with activities
	A17 Co-ordinate implementation of plans	Definition of a framework for the coordination of the NRM activities based on the risk options selected and	*Outputs of A16* **O.16.1** Risk treatment options according to risks (possibly classified according to the risk limits) **O.16.2** Action plan as sequence of prioritized activities (expressed as implementation of	**O.17.1** Coordination of activities **O.17.2** Progress reports from other projects **O.17.3** Progress reports from the implementation of measurements (e.g. from ISMS)

Process	Activity	Description	Inputs	Outputs
		the resources and responsibilities assigned. Dissemination of information related to the implementation of measurements and provision of costs' overview.	controls or as protection of assets) **O.16.3** Assignment of resources (e.g. costs) for action plan implementation **O.16.4** Assignment of responsibilities for each action **O.16.5** Approved lists with activities	**O.17.4** Overview of costs
Process 7: Risk Acceptance	**A18** Risk Acceptance	Final formal decisions for risk treatment based on the risk prioritisation.	**I.18.1** Formal decision about previously analysed risks and about which risks will be treated (and possibly with what priority) or left untreated	**O.18.1** Formal decision about the way risks have been treated
Process 8: Risk Communication and Awareness	**A19** Risk communication and awareness	Communication to internal and external partners and stakeholders. Establishment of risk communication plans.	**I.19.1** Reporting on incidents (external and internal) **I.19.2** Requests to inform Management arising from the risk treatment plan **I.19.3** Awareness information coming from relevant sources (e.g. internal directives and rules for processing and using information systems) **I.19.4** Consulting reports from experts (internal and external) **I.19.5** Requests for consulting on detailed security issues, or to perform an evaluation activity	**O.19.1** Communication to internal and external partners **O.19.2** Awareness information for all involved stakeholders **O.19.3** Consulting request to external specialists **O.19.4** Risk communication plan
Process 9: Monitor and review	**A20** Monitor and evaluate implementation progress	Monitoring and evaluation of the risk management process and reporting on internal and cost indicators. Reports on events to internal stakeholders and external parties.	**I.20.1** External reference documents e.g.: • Metrics methodologies • Incident data from CERTs • Information from dedicated security organizations (ENISA, ISACA, SANS, NIST, etc.) **I.20.2** Internal reference documents **I.20.3** Lists of Security Policies **I.20.4** Reports on incidents from business processes **I.20.5** Reports on incidents from national exercises	**O.20.1** Reports on events and consequences to internal stakeholders **O.20.2** Reports on events and consequences to external concerned parties (e.g. state agencies and stakeholders) **O.20.3** Internal indicators (e.g. KPIs) **O.20.4** Cost indicators **O.20.5** Lessons learned from implementation

Process	Activity	Description	Inputs	Outputs
			Output of A14 **O.14.1** List of relevant threats **O.14.2** List of relevant vulnerabilities of (groups of) assets **O.14.3** List of relevant impacts **O.14.4** List of values including frequency, severity and value of assets affected **O.14.5** Interdependencies between sectors *Output of A15* **O.15.1** Tables with assets classified according to the classification scheme **O.15.2** List of threats and vulnerabilities relative to each asset **O.15.3** List of existing controls relative to each asset (part of so-called gap analysis) **O.15.4** List of impacts relative to each asset **O.15.5** List of risks relative to each asset **O.15.6** Qualified or quantified risks relative to each asset or asset group (with consequences, likelihood, cumulative impact relative to each asset or asset group) **O.15.7** Formal decision about previously analysed risks and about which risks will be treated (and possibly with what priority) or left untreated	

Table 5: Processes, activities, inputs and outputs for individual risk management implementation

Annex C: NRM Governance Framework Questionnaire

In order to produce a high-level assessment of National Risk Management (NRM) preparedness, the ENISA Working Group has devised a questionnaire for use by either representatives of national governments or by representatives of regulatory bodies or of organisations that are major providers of critical information infrastructure. The purpose of this questionnaire is to give governments an assessment of their preparedness in the different activities of NRM; and thus the possible state of overall NRM preparedness in their country. The questionnaire is not intended to benchmark individual countries or to attempt comparisons between countries. The questionnaire is intended to be completed as a reflection of the opinion of the respondent.

Identification

First, please complete the section below, with an indication of the country about which you are completing the questionnaire and the type of organisation you represent.

Name*	
Country	
Organization*	
Which type of organization do you represent?	☐ National Government / relevant organization (i.e. parliament, ministries, etc.) ☐ National Security Institution ☐ Regulatory Body or Sector Association ☐ Individual Organization (company, public body, NGO, etc.)
Date	

* Optional

All information will be treated in the strictest confidence.

Using the Questionnaire

The questionnaire set out below is divided into 12 sections: one for each of the 12 activity groups (A1 to A12) shown in Figure 3 (section 7). Respondents should read the description given for each of the activity groups and then should look at the five statements below it. Each of these statements corresponds to a level of capability maturity within the activity group described. The statements are based on the model used by the Control Objectives in IT (COBIT) standard.

At the end of the section, the respondent should check the box that, in his or her opinion, most closely matches the level of maturity to be found in his or her country. If the respondent considers that the maturity level is intermediate between two descriptions – or has elements of two descriptions – this may be indicated by either checking two boxes or drawing a line between them.

If desired, the respondent may add a comment at the end of each section. For example to indicate why a particular box has been checked or to point out that the NRM governance situation about which he or she is reporting contains elements that are at a number of maturity levels – and that the checked box therefore represents an “average” value.

Process 1: Define NRM Policy

A1: Set the Vision

This activity takes into account political and legal decisions and requirements, as well as current NRM status, effectiveness and activities in relation to the protection of the critical information infrastructure, in order to set strategic goals and objectives for National Risk Management. It identifies key stakeholders and their ability to collaborate and contribute towards NRM outputs including regulation, goal setting and incentives for collaboration.

Maturity Level 1

Sporadic and ad-hoc account is taken of legal decisions and requirements, but no clear NRM policy is documented. Strategic goals and objectives are not set. Key stakeholders are not identified.

Maturity Level 2

Awareness of the need to take into account political and legal decisions and requirements leads to some NRM policy making. Some strategic goals set but these are inconsistent and ad-hoc. Some key stakeholders have been identified but are not co-ordinated.

Maturity Level 3

Political and legal decisions and requirements are documented and co-ordinated to create NRM policies, but these are not fully communicated or coordinated with current activities. Strategic goals are set but are not consistently applied or monitored. All key stakeholders are identified, but are not co-ordinated.

Maturity Level 4

Political and legal decisions and requirements and the current status and effectiveness of NRM activities are fully taken into account when setting documented and communicated NRM policies. Strategic goals are set and consistently applied and continuous improvement is emerging. Key stakeholders are identified and co-ordinated.

Maturity Level 5

There is a proactive and forward-looking approach to ensuring that political and legal decisions and requirements are related to NRM policy effectiveness and activities, and that these are fully documented. Strategic goals are fully integrated, monitored and measured to ensure their effective achievement. There is proactive identification and continuous update of key players.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A2: Establish NRM Organisation

This activity takes into account political, market and security requirements in order to assign roles, responsibilities and tasks to appropriate key stakeholders within the NRM framework. It assigns appropriate tasks and co-ordinates actions within and between groups to ensure effective NRM synergies. It uses appropriate information flow and communication mechanisms to ensure stakeholders and key players are effective in complying with legal and regulatory requirements and fulfilling assigned roles.

Maturity Level 1

Sporadic and ad-hoc notice is taken of political market and security requirements, but there is no formal and documented definition of key roles and responsibilities. Tasks in relation to NRM are assigned on an ad-hoc basis and there is no coordination between groups of stakeholders. Communication takes place sporadically, if at all and there is no mechanism for checking the effectiveness of activities by key players.

Maturity Level 2

Some notice is taken of the political, market and security requirements and this leads to informal responsibility for NRM actions being taken by individuals. Individuals are aware of their tasks in relation to NRM, but these are not consistently documented or communicated. Some communication and coordination takes place between groups, but this is not fully documented. Note is taken of activities, but this is not formal or consistent.

Maturity Level 3

Political, market and security requirements are used to define NRM roles and responsibilities, but individuals are not given full authority to act. Activities and tasks are formally defined for key responsibilities, but activities are not fully coordinated. Communication channels have been implemented, but these are not used consistently. Performance measures for activities have been formally defined, but these are applied inconsistently and not always used.

Maturity Level 4

Political, market and security requirements are used to ensure that appropriate key NRM roles and responsibilities are fully identified and that individuals are fully empowered to take effective action. Activities and tasks in relation to NRM are fully identified and defined and are effectively coordinated. Communication channels are well understood and consistently used. Defined performance measures are used to ensure that NRM activities appropriate to the defined roles are effectively carried out.

Maturity Level 5

There is a proactive and forward-looking approach to gathering political, market and security requirements for NRM, ensuring that roles and responsibilities for key stakeholders are continuously updated. Timely and effective identification of new and updated activities and tasks takes place where appropriate and these are fully communicated to well-coordinated groups of key stakeholders. Performance of responsibilities is continuously measured and performance improvement is a way of life.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Process 2: Coordinate and Support Implementation

A3: Support and Regulate

This activity provides an appropriate support and regulation framework that is fully aligned with dynamic NRM policies, strategic goals and identified key stakeholders, taking into account political, market and security conditions, in order to provide appropriate regulation for NRM activities performed by those with identified roles and responsibilities. These activities ensure that NRM information is fully and effectively shared between them.

Maturity Level 1

Support for NRM activities is sporadic and ad-hoc. There is no attempt to align activities with national policies, strategic goals and key stakeholders and no account is taken of political, market or security considerations. Regulation of NRM activities is not performed and NRM information is not shared.

Maturity Level 2

Some informal support is provided for NRM activities. Informal attempts are made to align activities with national policies, strategic goals and key stakeholders and some account is taken of political, market and security considerations. Regulation of NRM activities is informal and ad-hoc and information is shared only sporadically.

Maturity Level 3

There is clear support for NRM activities, but this is not always fully adequate. Support is aligned with national policies, strategic goals and key stakeholders, and account is taken of political, market and security considerations; but this is not always consistent. There is formal regulation of NRM activities, but this is not always fully communicated. Information sharing takes place but is not consistent.

Maturity Level 4

Full, clear and adequate support is given to all NRM activities. Support is fully aligned to national policies and strategic goals and political, market and security issues are always taken into full consideration. NRM activities are fully regulated within a clear framework, which is communicated to all stakeholders. NRM information is fully and effectively shared.

Maturity Level 5

Full clear and adequate support for all NRM activities is continuously adjusted to proactively meet changes in national policies, strategic goals and key stakeholders, as well as significant political, market and security developments. The regulatory framework for NRM activities is subject to continuous improvement as a result of effective communication with and between stakeholders. NRM information sharing is effective and monitored to ensure its ongoing value.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A4: Promote Awareness

This activity takes into account national policies and goals for awareness raising to develop effective material and programmes to train and educate clearly defined NRM participants and target groups. The effectiveness of the training material and programmes is monitored and measured and lessons are learned to ensure that continuous improvement takes place.

Maturity Level 1

Awareness raising is sporadic and ad-hoc and little account is taken of national policies and goals. NRM participants and target groups are not clearly identified. There is no monitoring and measurement of the effectiveness of training and education.

Maturity Level 2

Some awareness raising material and programmes are produced in response to national policies and goals. These are delivered to some NRM participants and groups on an informal basis. The effectiveness of training and education is measured inconsistently and sporadically.

Maturity Level 3

Clear awareness raising training and education programmes have been put in place in response to national policies and goals. However, the material these produce is not always fully supported. Appropriate NRM participants and target groups have been identified, but delivery of programmes is not always consistent. Monitoring and measurement of effectiveness takes place, but lessons are not always learned.

Maturity Level 4

Fully supported awareness raising education and training courses have been implemented to deliver clear and effective material to appropriate NRM participants and target groups in a consistent manner. The effectiveness of the training and education courses is monitored and measured and lessons are learned and incorporated into courses.

Maturity Level 5

Fully supported awareness raising and education courses are proactively and continuously adjusted to deliver optimum material to appropriately identified target groups of NRM participants as and when required. Monitoring and measurement of the value and effectiveness of awareness raising is continuous and improvement in the training and education courses takes place as soon as it is required.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A5: Provide Necessary Information

This activity gathers timely, relevant and appropriate information on technical risks (threats, vulnerabilities, incidents and impacts) to information systems, and on the effectiveness of the mitigation and management of those risks, from identified stakeholder organisations. This information is aggregated and analysed in order to deliver statistical data on the national risk landscape and to share information to assist in the effective and timely coordination of future risk management actions.

Maturity Level 1

Information gathering about technical risks and their mitigation and management is sporadic and ad-hoc. The information is received informally from organisations when they chose to give it. No formal data aggregation or analysis takes place and sharing of statistical or other risk-related information takes place informally, if at all.

Maturity Level 2

Some information about technical risks, their mitigation and management is gathered from a few identified stakeholder organisations. Information is aggregated and analysed sporadically and dissemination of statistical data and sharing of risk-related information takes place occasionally.

Maturity Level 3

Mechanisms are in place to gather information about technical risks, their mitigation and management, from clearly identified stakeholders. However, these are not always fully supported by participating organisations. Available information is aggregated and analysed according to a clear schedule and there is some structured dissemination of statistical and risk-related information.

Maturity Level 4

All appropriate stakeholder organisations fully participate in the sharing of information about technical risks, their mitigation and management. The information is frequently aggregated and analysed and clear and timely statistical reports are produced. Effective and timely risk-related information is shared with appropriate organisations.

Maturity Level 5

All stakeholder organisations proactively participate in the delivery of timely and relevant information about technical risks, their mitigation and management. The information is continuously aggregated, analysed in relation to all other factors of relevance and frequent national statistical reports are produced. Risk-related information is shared continuously between all participating stakeholders in order to ensure timely and effective risk management.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A6: Promote Standards

This activity gathers information on appropriate standards and best practices related to risk management preparedness. These are evaluated for their relevance and likely effectiveness in improving NRM methods. Existing NRM methods are adapted and updated accordingly. Key players in both public and private sectors are identified and information about new and improved standards and best practices and recommendations about adapted and updated methods are then disseminated to them. Checks are employed to ensure that they are used in a timely and effective manner.

Maturity Level 1

Information gathering about risk management preparedness best practices and standards is sporadic and ad-hoc. No consistent evaluation takes place and existing methods are updated sporadically, if at all. Information dissemination to ad-hoc recipients takes place inconsistently and informally, if at all.

Maturity Level 2

Some information is gathered about improvements to standards and best practices related to risk management preparedness and these are evaluated for their relevance to NRM methods. However, evaluation is inconsistent and informal and does not automatically result in updates to existing methods. Dissemination of information to some identified key players takes place, but this is not timely or coordinated.

Maturity Level 3

Information is regularly gathered about improvements to standards and best practices related to risk management preparedness. Evaluation is performed and existing NRM methods are updated as necessary. Key players are identified and information is disseminated regularly, but not necessarily in a timely or effective manner.

Maturity Level 4

Fully documented and formal methods are used to gather information about improvements to standards and best practices related risk management preparedness. Evaluation is performed on the gathered information and formal mechanisms are in place to updated existing NRM methods as a result. Information about new standards, best practices and updated NRM methods is disseminated to all key players in a timely and effective manner.

Maturity Level 5

Proactive and forward-looking measures are taken to encourage the improvement of best practices and standards relating to risk management preparedness and information is gathered. Evaluation is performed and existing methods are fully and effectively updated. Key players are continuously updated and information about the new best practices, standards and methods is rapidly disseminated to them in a timely and effective manner. Feedback is gathered to ensure that the best practices, standards and methods are appropriately and effectively deployed.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A7: Foster Collaboration

This activity identifies intra- and inter-sectoral interdependencies between identified key players. It analyses and evaluates them to determine appropriate responses, including coordinated risk management and self-regulation where necessary. Responses are appropriately disseminated and national exercises are carried out to ensure the effective and efficient operation of inter- and intra-sectoral collaboration.

Maturity Level 1

Information about inter- and intra-sectoral interdependencies is sporadic and ad-hoc. There is little or no evaluation of these and appropriate responses are not formally determined. There is little or no dissemination of information about interdependencies and exercises to test these are not carried out.

Maturity Level 2

Some information about inter-and intra-sectoral dependencies is gathered, but not necessarily fully documented. Appropriate responses to these interdependencies are determined informally and are communicated in an ad-hoc way to some of the key players. Exercises may be carried out, but these are sporadic and not fully coordinated.

Maturity Level 3

Information about inter- and intra-sectoral dependencies is gathered and documented. Some formal evaluation and determination of responses takes place and communication with key players takes place. Exercises to test the responses are carried out, but these are not fully coordinated and not all key players are always involved.

Maturity Level 4

Inter- and intra-sectoral interdependencies between all key players are identified and fully documented. Formal methods are used to analyse and evaluate these and to determine appropriate responses. Responses are disseminated to all key players and national exercises are carried out to test inter- and intra-sectoral collaboration.

Maturity Level 5

Proactive determination of inter- and intra-sectoral interdependencies is carried out as political, market and security conditions change. Formal methods are used to analyse and evaluate these and to determine appropriate responses, especially shared risk management. Proactive dissemination of collaboration advice and responses takes place and these are tested in a timely and effective way through fully coordinated national exercises.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A8: Monitor Effectiveness

This activity monitors and gathers information about the occurrence of events related to NRM and their consequences for those stakeholders involved. Reports are collated and analysed in relation to clearly defined, agreed NRM performance indicators. The effectiveness of NRM is assessed in the light of performance and, where necessary and appropriate, timely proposals for the adaptation of NRM methods and activities are made.

Maturity Level 1

Collection of information about the occurrence of NRM related events is sporadic and ad-hoc. Performance indicators for NRM are not set. Little or no assessment is made of NRM performance and no proposals are made to adapt NRM methods and activities.

Maturity Level 2

Some monitoring and collection of information about NRM related events takes place. Some informal performance indicators are set and reports about events may be analysed in relation to these. Informal proposals may be made to adapt and improve NRM methods and activities.

Maturity Level 3

Monitoring of NRM-related events takes place with some key stakeholders. Formal performance indicators have been set, but event reports are not always collated and analysed in relation to these. Where collation and analysis occurs, NRM effectiveness is assessed and, where appropriate, proposals may be made to adapt and improve NRM methods and activities.

Maturity Level 4

Monitoring and collection of NRM-related event information takes place with all key stakeholders. Formal performance indicators are fully communicated, and reports are always collated and analysed in relation to these to assess NRM performance effectiveness. Where appropriate, proposals will always be made for the improvement of NRM methods and activities.

Maturity Level 5

All key stakeholders are proactively monitored to detect NRM related event data. The data are collated and analysed in real-time in relation to updated and agreed performance indicators. Any loss of performance effectiveness is immediately detected and timely and effective proposals are made to ensure improvement of NRM methods and activities.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Process 3: Review, Reassess and Report

A9: Analyse Errors and Incidents

This activity monitors and collects information about security errors and incidents from CERT-type bodies within stakeholder organisations and from European and international cooperative schemes. Information about the efficiency and effectiveness of incident and error handling and response is collated and analysed in the light of NRM performance indicators and adaptation and improvement proposals (from A8). Useful and timely risk assessments are carried out for appropriate stakeholders, on request, on the basis of the reports and analysis. Collated reports and analysis concerning security error and incident handling are made and submitted to appropriate national authorities.

Maturity Level 1

Liaison with CERT-type bodies and European and international cooperative schemes is sporadic and ad-hoc. Information about security errors and incidents is collected occasionally, on an informal basis. Analysis, if carried out, is informal, not detailed and is not used for carrying out risk assessments. Reports may be produced for national authorities, but these are sporadic and ad-hoc.

Maturity Level 2

Liaison takes place with a number of CERT-type bodies and with European and international cooperative schemes. Information from these bodies and schemes is collected and may be informally analysed in the light of NRM performance indicators and adaptation and improvement proposals. Risk assessments may, occasionally be carried out for authorised stakeholders. Occasional reports are produced for national authorities.

Maturity Level 3

Formal liaison processes are in place to gather and collate information from CERT-type bodies and international cooperative schemes, but these are not actively pursued. Information gathered is analysed at infrequent intervals in the light of NRM performance indicators and adaptation and improvement proposals. Mechanisms are in place to allow authorised stakeholders to request risk assessments, but these are not widely communicated. Reports for national authorities are produced at least annually.

Maturity Level 4

Effective liaison with CERT-type groups and with European and international cooperative schemes ensures a steady flow of information about security errors and incidents. This is collated and analysed in the light of NRM performance indicators and adaptation and improvement proposals. This allows risk management reports to be produced for authorised stakeholders on request. Frequent reports based on the analysis are produced for national authorities.

Maturity Level 5

Proactive liaison with CERT-type bodies and European and international cooperative schemes results in immediate notification of information about security errors and incidents. Continuous monitoring and collation of this information flow allows immediate analysis in the light of up to date information about NRM performance and adaptation and improvement. This allows proactive risk assessments to be made in real-time for authorised stakeholders and real-time alerts and reports to be produced for national authorities.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A10: Review Effectiveness

This activity determines evaluation criteria and quality parameters for the effectiveness of NRM processes. It monitors information about NRM performance in response to incidents and issues. This is reviewed in the light of the performance criteria, evaluations based on organised survey data and on ongoing consultations with competent authorities. Audit reports are produced as a result of the review process and action plans based on the audit reports are documented and delivered.

Maturity Level 1

Evaluation criteria and quality parameters, where they exist, are sporadic and ad-hoc. Information about NRM performance is gathered informally and sporadically. Survey data is not gathered and consultations with competent authorities are occasional and informal. Audit reports and action plans are not produced.

Maturity Level 2

Some evaluation criteria and quality parameters have been produced. Information about NRM performance is gathered informally and may be analysed in relation to those evaluation criteria and quality parameters which exist. Some survey data is gathered sporadically and informal consultations with competent authorities take place. Audit reports and action plans may be produced, but these are infrequent.

Maturity Level 3

Evaluation criteria and quality parameters have been documented, but these are not necessarily fully communicated. Formal processes exist for gathering NRM performance information, but these are not always followed. Formal processes exist for gathering survey data and holding consultations with competent authorities, but again these are not always followed. Collation and analysis of the information takes place at least annually and audit reports are written. Action plans may be produced if necessary.

Maturity Level 4

Effective evaluation criteria and quality parameters are in place and fully communicated. NRM performance information is regularly gathered. Organised surveys are carried out regularly, as is consultation with competent authorities. NRM performance information is regularly evaluated in the light of evaluation criteria, quality parameters, survey data and the results of consultations. NRM audit reports are regularly produced, as are action plans for NRM performance improvement.

Maturity Level 5

Evaluation criteria and quality parameters are set and proactively updated in the light of the changing political, market and security landscape. NRM performance information is actively and continuously gathered. Surveys and consultation with competent authorities take place proactively and frequently. NRM performance information is continuously evaluated in the light of evaluation criteria, quality parameters, survey data and the results of consultation. NRM reports are produced dynamically and frequently and action plans for NRM performance improvement are issued in real-time.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A11: Report on NRM Process Maturity

This activity monitors the implementation of other NRM activities and gathers inputs including risk assessments for individual stakeholders, reports and analysis on security error and incident handling, reports on NRM process effectiveness and NRM improvement action plans. This information is collated and analysed to evaluate current NRM performance. On the basis of this analysis, current NRM preparedness status reports are produced and disseminated.

Maturity Level 1

Gathering of information from other NRM activities is sporadic and ad-hoc. Information is not formally analysed and evaluated. Informal NRM preparedness status reports may be produced sporadically, if at all.

Maturity Level 2

There is some organised gathering of information from other NRM activities. Information gathered is analysed and evaluated irregularly and NRM preparedness status reports are produced occasionally, but not to a regular schedule.

Maturity Level 3

Formal processes exist for the gathering of information from other NRM activities, but these are not always followed. Processes exist for the analysis and evaluation of the material, but again these are not always followed. NRM preparedness status reports are produced at intervals of longer than one year.

Maturity Level 4

Formal processes are used to monitor the production of information from other NRM activities and to gather them regularly. The material gathered is regularly analysed and evaluated. Effective NRM preparedness status reports are produced at a frequency of at least once a year.

Maturity Level 5

Continuous monitoring and gathering of information from other NRM activities takes place. The material gathered is continuously analysed and evaluated. Timely and effective NRM preparedness reports are produced, both regularly and in response to particular political, market or security issues.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A12: Suggest Improvements

This activity monitors and gathers NRM preparedness status reports. These are collated and analysed in relation to the overall picture of the critical information infrastructure (CII). On the basis of the analysis timely and effective action plans are produced to ensure the ongoing improvement of NRM preparedness.

Maturity Level 1

NRM preparedness status reports are received sporadically and on an ad-hoc basis. There is no attempt to analyse these in relation to the overall CII picture. Coherent action plans are not produced.

Maturity Level 2

Information is gathered from the few NRM preparedness status reports that are available. Some informal analysis of these in relation to the overall CII picture takes place. Action plans may be produced, but these are incomplete and sporadic.

Maturity Level 3

Processes exist to gather information from the available NRM preparedness status reports, but these are not always followed. Processes exist for the analysis of this information in relation to the overall CII picture, but again these are not always followed. Action plans are produced at intervals, but these tend to be incomplete.

Maturity Level 4

Information produced by other NRM activities is monitored and gathered regularly. The information gathered is regularly analysed in relation to the overall CII picture. Action plans for the improvement of NRM preparedness are regularly produced.

Maturity Level 5

Other NRM activities are continuously monitored and information is gathered. The information gathered is continuously analysed in relation to the overall CII picture, which is continuously updated. Timely and effective action plans are produced that are targeted in response to particular political, market or security issues.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Annex D: Questionnaire for CII Stakeholder Organisations

To assist with the high-level assessment of National Risk Management (NRM) preparedness, the ENISA Working Group has devised a questionnaire for use by representatives of CII stakeholder organisations. The purpose of the data from this questionnaire is to assist governments in understanding the effectiveness of their NRM processes from the point-of-view of CII stakeholders. The questionnaire is intended to highlight those areas where coordination of, and communication with stakeholders could be further developed or improved. It is not intended to benchmark individual countries or to attempt comparisons between countries. The questionnaire is intended to reflect the awareness of the respondent concerning their government's NRM activities.

Identification

First, please complete the section below, with an indication of the country about which you are completing the questionnaire and the type of organisation you represent.

Name*	
Country	
Organization*	
Which type of organization do you represent?	☐ ICT services provision ☐ ICT hardware or software provision ☐ Law enforcement ☐ NGO or representative organisation
Date	

* Optional

All information will be treated in the strictest confidence.

Using the Questionnaire

The questionnaire set out below is divided into 12 sections: one for each of the 12 activity groups (A1 to A12) shown in Figure 3 (section 7). Respondents should read the description given for each of the activity groups and then should look at the five statements below it. Each of these statements corresponds to a level of delivery which they might expect from their government. The statements are based on the capability maturity model used by the Control Objectives in IT (COBIT) standard.

At the end of the section, the respondent should check the box that, in his or her opinion, most closely corresponds to the level of government delivery of which the respondent is aware. If the respondent considers that the level is intermediate between two descriptions – or has elements of two descriptions – this may be indicated by either checking two boxes or drawing a line between them.

If desired, the respondent may add a comment at the end of each section. For example to indicate why a particular box has been checked or to point out that the government delivery about which he or she is reporting contains elements that are at a number of maturity levels – and that the checked box therefore represents an "average" value.

Process 1: Define NRM Policy

A1: Set the Vision

This activity takes into account political and legal decisions and requirements, as well as current NRM status, effectiveness and activities in relation to the protection of the critical information infrastructure, in order to set strategic goals and objectives for National Risk Management. It identifies key stakeholders and their ability to collaborate and contribute towards NRM outputs including regulation, goal setting and incentives for collaboration.

Maturity Level 1

Government has no clear NRM policy and strategic goals and objectives have not been set. No key stakeholders have been identified.

Maturity Level 2

Government has set some NRM policies and strategic goals set; but these are inconsistent and ad-hoc. Some key stakeholders have been identified, but their activities are not co-ordinated.

Maturity Level 3

Government has set NRM policies and strategic goals, but they have not been fully communicated to you; nor are they consistently coordinated and managed. All key stakeholders have been identified, but their actions are not co-ordinated.

Maturity Level 4

Government has given you full awareness of NRM policies and strategic goals. These are consistently applied and subject to continuous improvement with key stakeholders being well co-ordinated.

Maturity Level 5

Government ensures that NRM policies, strategic goals, activities, key players and their effectiveness are continuously monitored, updated and improved.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A2: Establish NRM Organisation

This activity takes into account political, market and security requirements in order to assign roles, responsibilities and tasks to appropriate key stakeholders within the NRM framework. It assigns appropriate tasks and co-ordinates actions within and between groups to ensure effective NRM synergies. It uses appropriate information flow and communication mechanisms to ensure stakeholders and key players are effective in complying with legal and regulatory requirements and fulfilling assigned roles.

Maturity Level 1

Government has not identified key NRM roles and responsibilities. Ad-hoc tasks may be assigned, but are not coordinated or monitored.

Maturity Level 2

Government has identified some NRM roles and responsibilities and assigned them; actions are undertaken informally, but these are not consistently documented, communicated, coordinated or monitored.

Maturity Level 3

Government has defined NRM roles, responsibilities activities and tasks, but individuals act without full authority and coordination. Communication and performance measurement is inconsistent.

Maturity Level 4

Government has fully defined NRM roles, responsibilities activities and tasks and these are authorised and coordinated. Communication and performance measurement ensure that NRM activities are effective.

Maturity Level 5

Government proactively updates and continuously coordinates NRM roles, responsibilities activities and tasks to ensure that performance improvement is ongoing.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Process 2: Coordinate and Support Implementation

A3: Support and Regulate

This activity provides an appropriate support and regulation framework that is fully aligned with dynamic NRM policies, strategic goals and identified key stakeholders, taking into account political, market and security conditions, in order to provide appropriate regulation for NRM activities performed by those with identified roles and responsibilities. These activities ensure that NRM information is fully and effectively shared between them.

Maturity Level 1

Government initiated NRM activities are sporadic, ad-hoc and unregulated. NRM information is not shared.

Maturity Level 2

Government initiated NRM activities are informally supported and regulated. NRM information is shared only sporadically.

Maturity Level 3

Government support for NRM activities is clear but not always adequate. Formal regulation of NRM activities and information sharing takes place, but this is not consistent.

Maturity Level 4

Government initiated NRM activities are fully supported and clearly regulated. NRM information is fully and effectively shared.

Maturity Level 5

Government initiated NRM activities and regulations are proactively adjusted to meet changing conditions and are continuously improved. NRM information sharing is monitored to ensure its ongoing value.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A4: Promote Awareness

This activity takes into account national policies and goals for awareness raising to develop effective material and programmes to train and educate clearly defined NRM participants and target groups. The effectiveness of the training material and programmes is monitored and measured and lessons are learned to ensure that continuous improvement takes place.

Maturity Level 1

Government NRM awareness raising, training and education is sporadic and ad-hoc with no monitoring and measurement of its effectiveness.

Maturity Level 2

Government NRM awareness raising, training and education are delivered informally, with effectiveness measurement inconsistent and sporadic.

Maturity Level 3

Government NRM awareness raising, training and education takes place, but delivery is not consistent. Monitoring and measurement of effectiveness takes place, but lessons are not always learned.

Maturity Level 4

Government NRM awareness raising, training and education is clear, effective and consistent. Monitoring and measurement of effectiveness takes place and lessons are learned and incorporated.

Maturity Level 5

Government NRM awareness raising, training and education is proactively and continuously adjusted. Monitoring and measurement is continuous and improvement takes place as soon as it is required.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A5: Provide Necessary Information

This activity gathers timely, relevant and appropriate information on technical risks (threats, vulnerabilities, incidents and impacts) to information systems, and on the effectiveness of the mitigation and management of those risks, from identified stakeholder organisations. This information is aggregated and analysed in order to deliver statistical data on the national risk landscape and to share information to assist in the effective and timely coordination of future risk management actions.

Maturity Level 1

There is no requirement from government to share information on technical risks. Ad-hoc analysis from government may be received.

Maturity Level 2

Government ensures that some information on technical risks is informally shared. Occasional government analysis is received.

Maturity Level 3

Government has implemented a mechanism to share information on technical risks, but this does not always operate effectively. Some structured government analysis and advice is received

Maturity Level 4

Government ensures that information on technical risks is shared effectively. Timely statistical reports and effective analysis of risk-related information is received from government.

Maturity Level 5

Government ensures that information on technical risks is gathered continuously. Proactive and valuable reports and analysis are received from government.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A6: Promote Standards

This activity gathers information on appropriate standards and best practices related to risk management preparedness. These are evaluated for their relevance and likely effectiveness in improving NRM methods. Existing NRM methods are adapted and updated accordingly. Key players in both public and private sectors are identified and information about new and improved standards and best practices and recommendations about adapted and updated methods are then disseminated to them. Checks are employed to ensure that they are used in a timely and effective manner.

Maturity Level 1

Information from government on standards and best practices is received sporadically and ad-hoc.

Maturity Level 2

Informal information from government on standards and best practices is received, but is not regularly published or necessarily timely or fully evaluated.

Maturity Level 3

Information from government on standards and best practices is received regularly, but is not always appropriate or timely.

Maturity Level 4

Information from government on standards and best practices, as well as updated methods, are published regularly and in a timely and effective manner.

Maturity Level 5

Government encourages the publication of proactive improvements in standards and best practices and continuously measures their effectiveness.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A7: Foster Collaboration

This activity identifies intra- and inter-sectoral interdependencies between identified key players. It analyses and evaluates them to determine appropriate responses, including coordinated risk management and self-regulation where necessary. Responses are appropriately disseminated and national exercises are carried out to ensure the effective and efficient operation of inter- and intra-sectoral collaboration.

Maturity Level 1

Government may gather information about interdependencies, but in a sporadic and ad-hoc way. No information is disseminated and no exercises to test these are carried out.

Maturity Level 2

Some information is gathered by government; informal communication about interdependencies may take place and sporadic exercises may be carried out.

Maturity Level 3

Information about interdependencies is formally gathered by government, some communication takes place and exercises are carried out, but not fully coordinated.

Maturity Level 4

Information about interdependencies is formally gathered by government and effective exercises are carried out to test inter- and intra-sectoral collaboration.

Maturity Level 5

Proactive determination of interdependencies is carried out by government in response to change and proactive national exercises take place to fully test responses.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A8: Monitor Effectiveness

This activity monitors and gathers information about the occurrence of events related to NRM and their consequences for those stakeholders involved. Reports are collated and analysed in relation to clearly defined, agreed NRM performance indicators. The effectiveness of NRM is assessed in the light of performance and, where necessary and appropriate, timely proposals for the adaptation of NRM methods and activities are made.

Maturity Level 1

Government collects sporadic and ad-hoc information about NRM related events and does not make any recommendations about improvements to NRM event responses.

Maturity Level 2

Government collects some information about NRM related events and may make Informal proposals to adapt and improve NRM event responses.

Maturity Level 3

Government undertakes formal collection of information about NRM-related events. Response effectiveness may be assessed and, where appropriate, proposals may be made for improvement.

Maturity Level 4

Government monitors and collects information about NRM events and response performance. Where appropriate, proposals are made for improvement.

Maturity Level 5

Government undertakes proactive, real-time monitoring of NRM events and responses and timely and effective recommendations for response improvement are made.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Process 3: Review, Reassess and Report

A9: Analyse Errors and Incidents

This activity monitors and collects information about security errors and incidents from CERT-type bodies within stakeholder organisations and from European and international cooperative schemes. Information about the efficiency and effectiveness of incident and error handling and response is collated and analysed in the light of NRM performance indicators and adaptation and improvement proposals (from A8). Useful and timely risk assessments are carried out for appropriate stakeholders, on request, on the basis of the reports and analysis. Collated reports and analysis concerning security error and incident handling are made and submitted to appropriate national authorities.

Maturity Level 1

No reports are received from government.

Maturity Level 2

Occasional reports may be received from government.

Maturity Level 3

Reports are received from government at least annually.

Maturity Level 4

Frequent reports are issued by government.

Maturity Level 5

Proactive reports are issued by government.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A10: Review Effectiveness

This activity determines evaluation criteria and quality parameters for the effectiveness of NRM processes. It monitors information about NRM performance in response to incidents and issues. This is reviewed in the light of the performance criteria, evaluations based on organised survey data and on ongoing consultations with competent authorities. Audit reports are produced as a result of the review process and action plans based on the audit reports are documented and delivered.

Maturity Level 1

Government does not review effectiveness of NRM actions or conduct surveys.

Maturity Level 2

Government informally reviews the effectiveness of NRM actions and surveys may be carried out sporadically.

Maturity Level 3

Government formally, but irregularly, gathers NRM performance information and surveys are sometimes carried out.

Maturity Level 4

Government regularly gathers NRM performance information and organised surveys are carried out.

Maturity Level 5

Government actively and continuously gathers NRM performance information. Surveys take place proactively and frequently.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A11: Report on NRM Process Maturity

This activity monitors the implementation of other NRM activities and gathers inputs including risk assessments for individual stakeholders, reports and analysis on security error and incident handling, reports on NRM process effectiveness and NRM improvement action plans. This information is collated and analysed to evaluate current NRM performance. On the basis of this analysis, current NRM preparedness status reports are produced and disseminated.

Maturity Level 1

Government does not issue NRM preparedness status reports; or if it does, these are informal.

Maturity Level 2

Government issues occasional NRM preparedness status reports.

Maturity Level 3

Government issues NRM preparedness status reports at intervals greater than one year.

Maturity Level 4

Government issues NRM preparedness status reports at least once a year.

Maturity Level 5

Government issues NRM preparedness status reports both regularly and in response to particular political, market or security issues.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

A12: Suggest Improvements

This activity monitors and gathers NRM preparedness status reports. These are collated and analysed in relation to the overall picture of the critical information infrastructure (CII). On the basis of the analysis timely and effective action plans are produced to ensure the ongoing improvement of NRM preparedness.

Maturity Level 1

Government does not issue coherent NRM action plans.

Maturity Level 2

Government issues incomplete and sporadic NRM action plans.

Maturity Level 3

Government issues NRM action plans at intervals, but these tend to be incomplete.

Maturity Level 4

Government issues regular NRM action plans.

Maturity Level 5

Government issues frequent, timely and up-to-date NRM action plans.

Maturity Level Assessment

Level 1	Level 2	Level 3	Level 4	Level 5

COMMENT

Annex E: Microsoft Excel Spreadsheet For Questionnaire Data Analysis

The spreadsheet which has been made available to accompany this report enables the analysis of data on capability maturities gathered from organisations involved in the protection of national CII, as well as allowing the results to be displayed graphically. It also enables multiple sets of results to be analysed to provide further graphical comparisons. The spreadsheet is designed to either be used stand-alone, or in conjunction with the questionnaires found in Annex C and Annex D of this document.

Use of the Spreadsheet

Respondents should first complete the "Identification" sheet, using the drop-down menu to select their organisation type.

Clicking on "Next" will take the respondent to the "Activity Maturity" tab. Figure 9 shows this section of the spreadsheet, where the respondent's assessments are entered. Maturity levels are as shown in the questionnaire at Annex C. Each maturity level is entered using a dropdown box.

Please note that if "Individual Organisation" is selected from the drop-down menu in the "Identification" sheet, the "Maturity Descriptions" that will be present are those relating to CII stakeholder expectations (see the questionnaire at Annex D).

National Risk Management Preparedness Questionnaire

					Maturity Descriptions			
	Activity	Name	Description	Maturity Level	Level 1	Level 2	Level 3	Level 4
Process 1 National Risk Management Policy Making	A1	Set the Vision	This group of activities takes into account political and legal decisions and requirements, as well as current NRM status, effectiveness and activities in relation to the protection of the critical information infrastructure, in order to set strategic goals and objectives for National Risk Management. Identifies key stakeholders and their ability to collaborate and contribute towards NRM outputs including regulation, goal setting and incentives for collaboration.	1.5	Sporadic and ad-hoc account is taken of legal decisions and requirements, but no clear NRM policy is documented. Strategic goals and objectives are not set. Key stakeholders are not identified.	Awareness of the need to take into account political and legal decisions and requirements leads to some NRM policy making. Some strategic goals set but these are inconsistent and ad-hoc. Some key stakeholders have been identified but are not co-ordinated.	Political and legal decisions and requirements are documented and co-ordinated to create NRM policies, but these are not fully communicated or coordinated with current activities. Strategic goals are set but are not consistently applied or monitored. All key stakeholders are identified, but are not co-ordinated.	Political and legal decision requirements and the curre effectiveness of NRM act taken into account when s documented and commun policies. Strategic goals ar consistently applied and co improvement is emerging. stakeholders are identified ordinated.
	A2	Establish NRM Organisation	This group of activities takes into account political, market and security requirements in order to assign roles, responsibilities and tasks to appropriate key stakeholders within the NRM framework. Assigns appropriate tasks and co-ordinates actions within and between groups to ensure effective NRM synergies. Uses appropriate information flow and communication mechanisms to ensure stakeholders and key players are effective in complying with legal and regulatory requirements and fulfilling assigned roles.	2.5	Sporadic and ad-hoc notice is taken of political market and security requirements, but there is no formal and documented definition of key roles and responsibilities. Tasks in relation to NRM are assigned on an ad-hoc basis and there is no coordination between groups of stakeholders. Communication takes place sporadically, if at all and there is no mechanism for checking the effectiveness of activities by key players.	Some notice is taken of the political, market and security requirements and this leads to informal responsibility for NRM actions being taken by individuals. Individuals are aware of their tasks in relation to NRM, but these are not consistently documented or communicated. Some communication and coordination takes place between groups, but this is not fully documented. Note is taken of activities, but this is not formal or consistent.	Political, market and security requirements are used to define NRM roles and responsibilities, but individuals are not given full authority to act. Activities and tasks are formally defined for key responsibilities, but activities are not fully coordinated. Communication channels have been implemented, but these are not used consistently. Performance measures for activities have been formally defined, but these are applied inconsistently and not always used.	Political, market and secu requirements are used to e appropriate key NRM role responsibilities are fully ide individuals are fully empow effective action. Activities relation to NRM are fully ic defined and are effectively Communication channels understood and consisten Defined performance mea to ensure that NRM activit to the defined roles are eff out.
	A3	Support and regulate	This group of activities provides an appropriate support and regulation framework that is fully aligned with dynamic NRM policies, strategic goals and identified key stakeholders, taking into account political, market and security conditions, in order to provide appropriate regulation for NRM activities performed by those with identified roles and responsibilities. These activities	2.5	Support for NRM activities is sporadic and ad-hoc. There is no attempt to align activities with national policies, strategic goals and key stakeholders and no account is taken of political, market or security considerations. Regulation of NRM activities is not performed and NRM information is not shared.	Some informal support is provided for NRM activities. Informal attempts are made to align activities with national policies, strategic goals and key stakeholders and some account is taken of political, market and security considerations. Regulation of NRM activites is informal and ad-hoc and information is shared only sporadically.	There is clear support for NRM activities, but this is not always fully adequate. Support is aligned with national policies, strategic goals and key stakeholders, and account is taken of political, market and security considerations; but this is not always consistent. There is formal regulation of NRM activities, but this is not always fully communicated.	Full, clear and adequate su to all NRM activities. Supp aligned to national policies goals and political, market issues are always taken int consideration. NRM activi regulated within a clear fran is communicated to all sta NRM information is fully a

Figure 9: Entering Questionnaire Data

After entering the data, the 'Next' button is pressed to go to the next page of the spreadsheet where the results are shown graphically, See Figure 10.

While the spreadsheet can be used with just a single set of results, the data can also be copied from this page in the spreadsheet using the 'Copy Data' function, see Figure 11. Thus multiple sets of results from a number of respondents in a single country can be collected. When the data is copied it can be input into the "Single Country Analysis" spreadsheet page, see Figure 12.

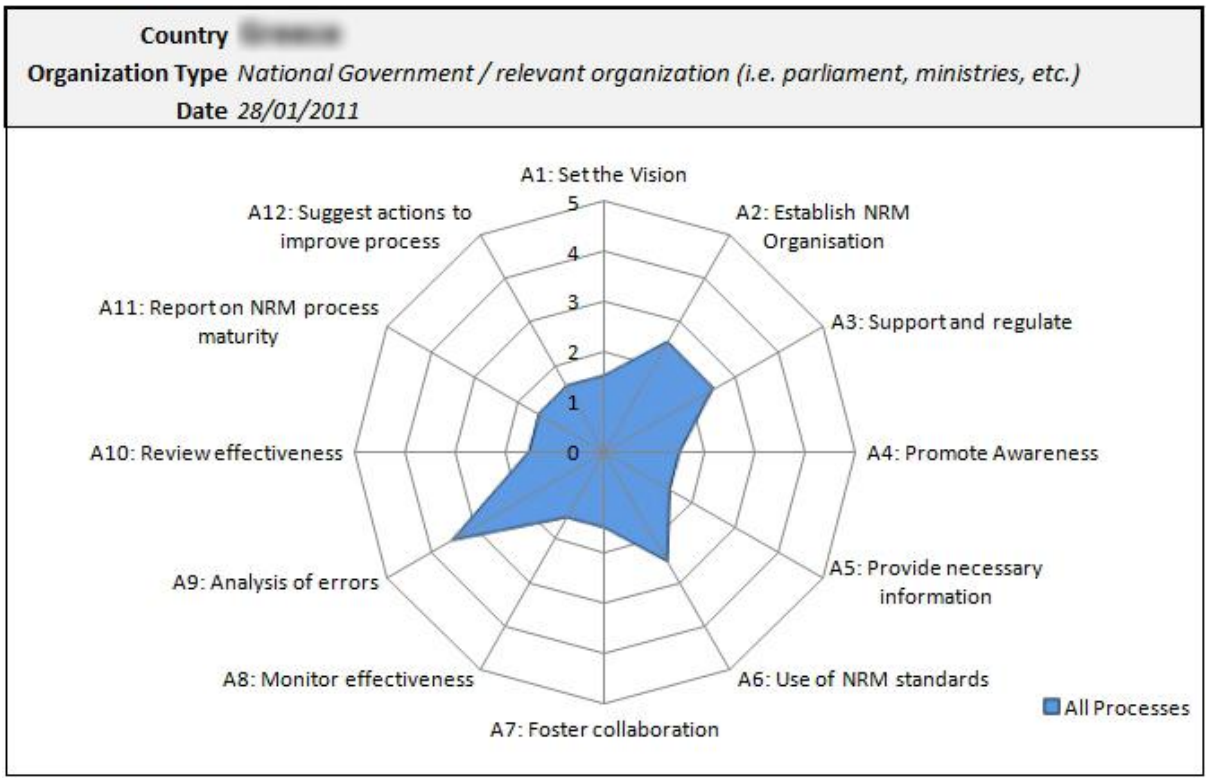

Figure 10: Questionnaire Results

	Copy Data
Country#	11
Org.#	1
A1	1.5
A2	2.5
A3	2.5
A4	1.5
A5	1.5
A6	2.5
A7	1.5
A8	1.5
A9	3.5
A10	1.5
A11	1.5
A12	1.5

Figure 11: Copy Questionnaire Data

Single Country Analysis

	Count	Average	Results 1	2	3	4	5	6	7	8	9	10
Country		11	11	11	11							
Organization		1	1	1	1							
A1: Set the Vision	3	1.83	1.5	1.5	2.5							
A2: Establish NRM Organisation	3	2.50	2.5	2.5	2.5							
A3: Support and regulate	3	2.50	2.5	2.5	2.5							
A4: Promote Awareness	3	2.00	1.5	1.5	3							
A5: Provide necessary information	3	2.00	1.5	1.5	3							
A6: Use of NRM standards	3	2.83	3	2.5	3							
A7: Foster collaboration	3	2.00	1.5	1.5	3							
A8: Monitor effectiveness	3	2.00	1.5	1.5	3							
A9: Analysis of errors	3	2.67	1.5	3.5	3							
A10: Review effectiveness	3	2.00	1.5	1.5	3							
A11: Report on NRM process maturity	3	2.00	1.5	1.5	3							
A12: Suggest actions to improve process	3	2.00	1.5	1.5	3							

Figure 12: Single Country Analysis

Single country analysis is an aggregation and averaging of individual sets of results to give a more complete picture of preparedness for the whole country, see Figure 13.

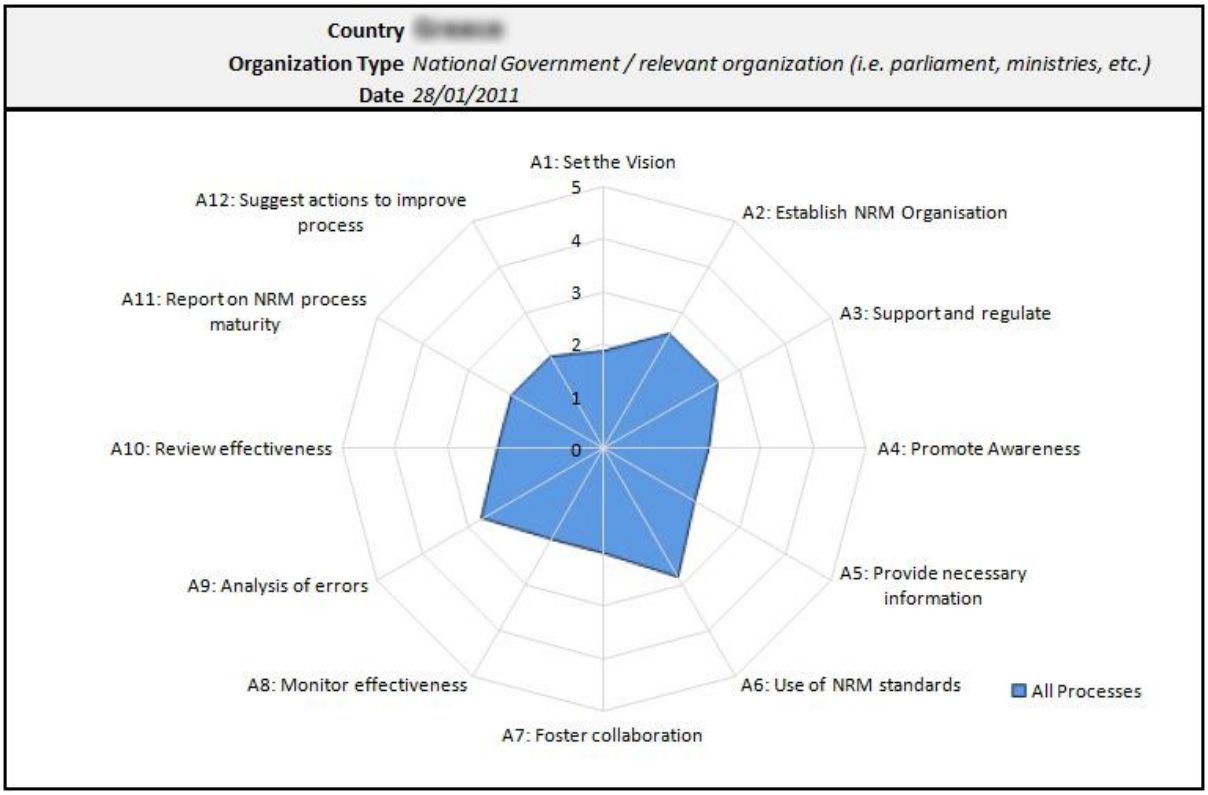

Figure 13: Single Country Combined Results

Finally, using a similar method of copying data from the single country results, the single country average data can be entered into the multiple country analysis spreadsheet page. This creates a comparison of the results across a (current) maximum ten different countries along with the average, see Figure 14.

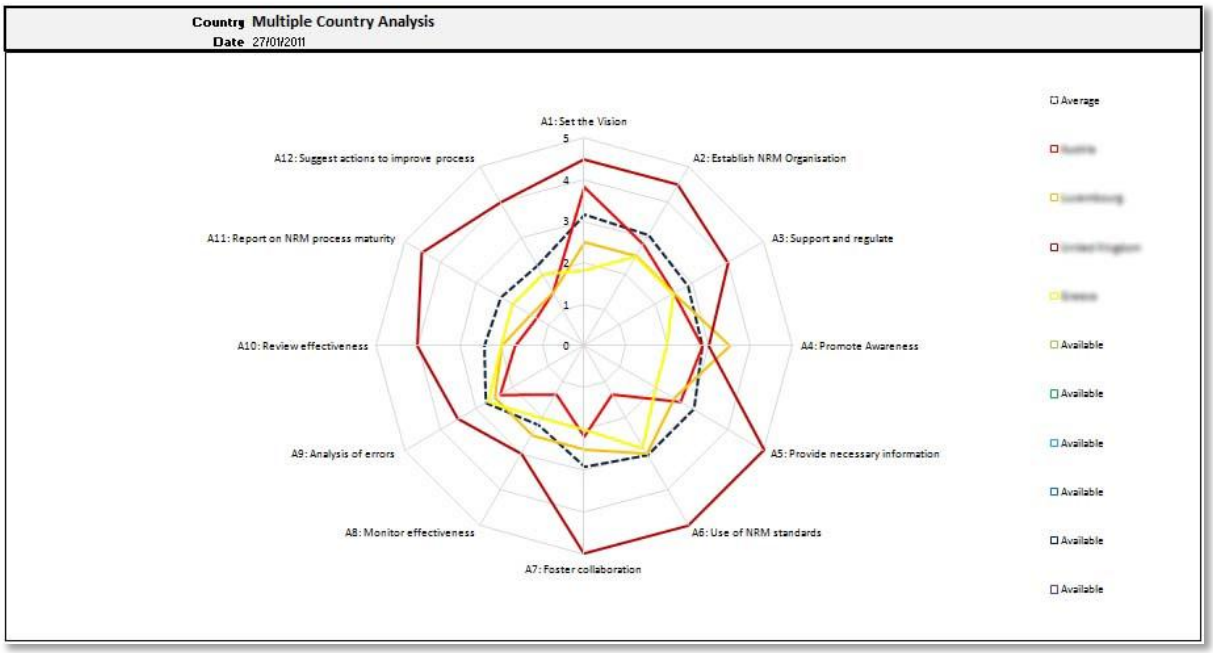

Figure 14: Multiple Country Results