EFR FRAMEWORK HANDBOOK

DRAFT

In cooperation with ATOS Origin Spain

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For more information on the EFR Framework, you may contact:

Barbara DASKALA Barbara.DASKALA@enisa.europa.eu
Dr. Louis MARINOS Louis.MARINOS@enisa.europa.eu

Contents

About this Handbook

The European Network and Information Security Agency (ENISA) seeks to assist the European Commission and the EU Member States, and in consequence cooperates with the business community, in order to help them meet the requirements of network and information security, thereby ensuring the smooth functioning of the internal Market, encompassing those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

According to Article 3 (a) of Regulation 2004/4602 ENISA fulfils the task to collect appropriate information in order to analyse current and emerging risks (Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJL 77, 13 March 2004, Article 3a). It concentrates on risks at the European level, which could produce an impact on the resilience and the availability of electronic communications networks as well as on the authenticity, integrity and confidentiality of the information accessed and transmitted through them.

This handbook in particular encompasses a documentation of the EFR Framework (Emerging and Future Risks Framework) which consists of a scenario-based process model developed in order to assess and manage emerging and future risks.

Generally the handbook should serve as a suitable guidance for anyone who wants to asses Emerging and Future Risks giving a comprehensive explanation of the EFR Framework. Particularly it ought to supply a reference for all involved groups in the EFR Framework appropriately documenting all the steps one needs to take in order to implement it. The involved participants could be Member States concerned about the impact of new technologies/applications which might implicate the need to introduce new or amended policy, the European Commission, consumer organisations, non-governmental organisations (NGOs), etc.

Apart from this, the handbook could be understood as a guideline to assist the EFR stakeholders and as a support for ENISA (European Network and Information Security Agency) on the EFR activities.

The handbook will be presented in four main parts:

- The first chapter mainly provides **introductory background information** about ENISA and its EFR roadmap initialized in 2006.
- The following chapter encloses a characterization of **organisational and implementation aspects** required in order to proceed and maintain the EFR Framework.
- The third part contains the major part of the handbook which encloses the presentation of the **EFR Framework**. The objective of the EFR Framework is the assessment and treatment of emerging and future risks by means of a systemized scenario-based process model. This includes the depiction of tasks and specific activities pertinent to each stage of the process, the corresponding roles and responsibilities as well as the information support which would be required.

- Finally, in the last chapter is presented a procedure for the **Maintenance of the EFR Framework** comprising a set of activities which would be required to keep the content updated.

1. Introduction

1.1. The EFR Framework: Scope and Objectives

In order to complement the existing initiatives in the area of addressing EFR, the Agency planned in 2008 to put the results of the already accomplished work into practice and to provide added value. Accordingly ENISA elaborated a structured approach towards identifying, assessing and managing emerging and future risks. The result is the development of the EFR Framework which will be documented more precisely in Part III of the present handbook.

The EFR Framework is an approach to systematize and automate the treatment of Emerging and Future Risks. In this Framework, requests may be submitted for an opinion on the emerging and future risks that might result from a combination of new technology and/or new applications being implemented. This may be from:

- Member States considering the impact of new technology/applications and the need for introducing new or amended policy
- The EC and other EU institutions considering the impact of strategic IS/IT planning or considering the development/implementation of new and innovative applications or technology

1.2. Assumptions and limitations

There are a number of assumptions and limitations which have to be considered during the performance of the EFR Framework.

- The EFR Framework is still in progress, in the sense that it will continue to be validated and improved in the year to come. This implies that the process can undergo modifications and will be updated accordingly during the next year.

- Existing RM/RA Methods focusing on current risks are followed in order to assess emerging and future risks during the Risk Management stage of the EFR Framework. Some of the existing assessment methodologies are more explicitly described on the ENISA website (http://www.enisa.europa.eu/rmra/rm_ra_methods.html)

- Apart from that, while ideas and proposals for topics to consider in the requests within the EFR Framework can be submitted by any stakeholder (industry, academia, EU Institutions etc.), specific requests to ENISA may only be submitted by EU Member States, the EC and other EU institutions.

1.3. Background information

The development of the framework has been an on-going process for the last two years. In this section, a brief overview of past activities leading up to the current state of the EFR

framework is presented. In 2006, ENISA provided an indicative *roadmap* (see ENISA website http://www.enisa.europa.eu) to address the issue of contemporary, emerging and future risk in risk management. In accordance with this roadmap, options for the collection and dissemination of information related to emerging and future risks were investigated and a study on this subject was delivered. Further to the above, in a study conducted in 2007, ENISA has begun to develop an appropriate method for the identification and management of Emerging and Future Risks.

In the increasingly interconnected global economy with its growing reliance on computers and networks in almost every aspect of human life, tolerance for risks that may disrupt the proper functioning of the digital backbone is shrinking. The demand for effective methods to manage emerging and future risks is climbing the list of priorities for most organisations. The accelerated pace of development of new technologies and applications poses a significant challenge to the management of the risks that may arise from the application of these technologies. Tackling this challenge requires the adaptation of current risk assessment and management methods to deal with emerging and future risks.

ENISA considers the following categorisation of risks in terms of timeframe:

- *Current Risks:* Risks that from a risk management point of view are relevant within the timeframe of present time up to one year.
- *Emerging Risks*: Risks that from a risk management point of view are relevant from one year to five years.
- *Future Risks:* Risks that from a risk management point of view are relevant beyond five years.

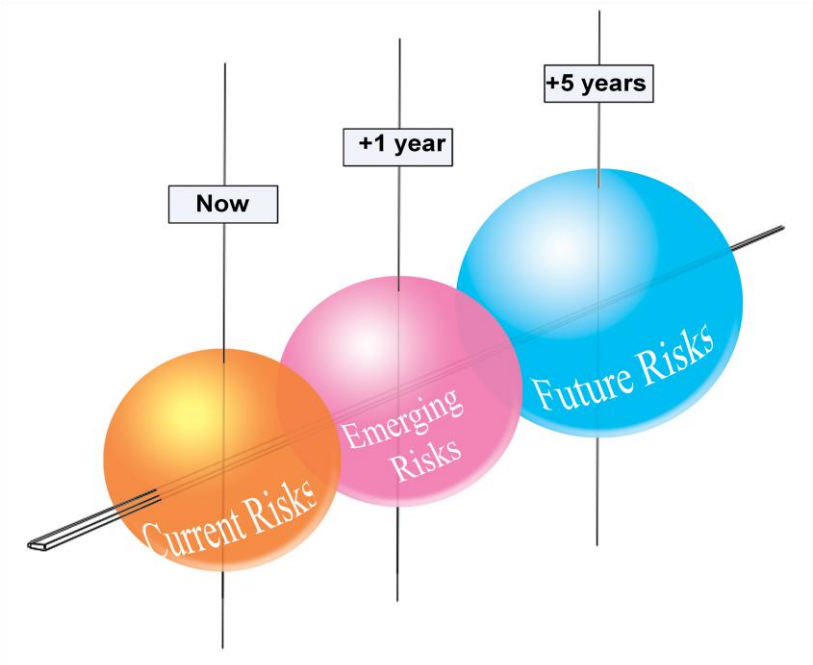

Figure 2: Categorisation of risks in terms of timeframe

Emerging and Future Risks are those that arise from either new applications based on existing technology, or existing applications implemented on new technology. According to the categorisation above, they will generally fall in the timescale from 1 to 5 years into the future. Future risks are those that arise from the implementation of new applications on new technology. These are generally in the time frame from 5 years and into the future. An illustration of these concepts can be found in the following image:

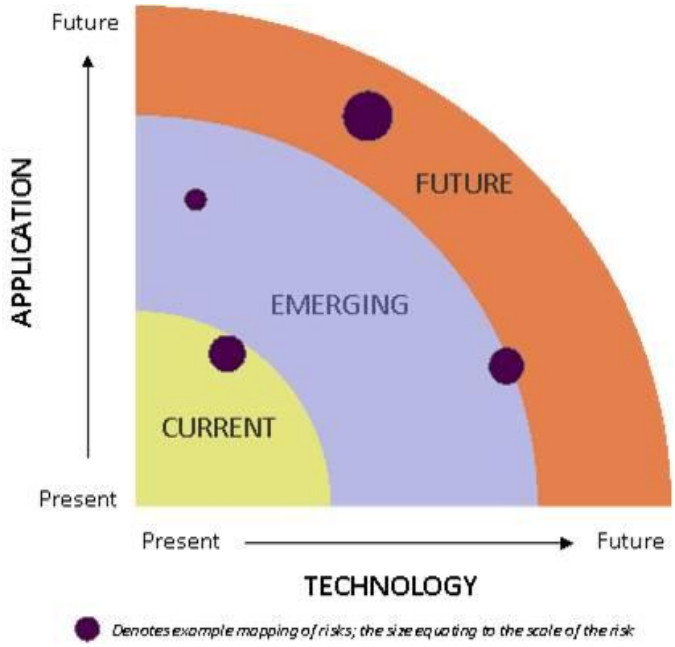

Figure 3: Emerging and Future Risks vs. Applications/Technology

The task was to develop an appropriate understanding of the requirements for **tackling emerging and future risks**, and to evaluate current risk assessment and management methods for their suitability. The starting point for developing Emerging and Future Risks was the evaluation of existing Risk Management/Risk Assessment methods in terms of their capability and suitability to identify and manage EFR, taking into account the specific nature of theses new risks. As an outcome the approach revealed that a number of modules/elements were missing.

Based on the results of this assessment, a detailed requirements definition document was produced that establishes the foundation for the extension and development of current or new methods to deal with emerging and future risk.

In a further step, a possible **extension** of existing **methods** for emerging and future risks was formulated. To provide maximum flexibility and to facilitate the integration of emerging and future risk assessment and management into existing methods, a modular approach was taken which foresees clearly defined stages and interfaces. The figure below depicts the stages of the developed module to satisfy the requirements for dealing with emerging and future risks. The module uses scenario generation to identify, analyse and understand risks.

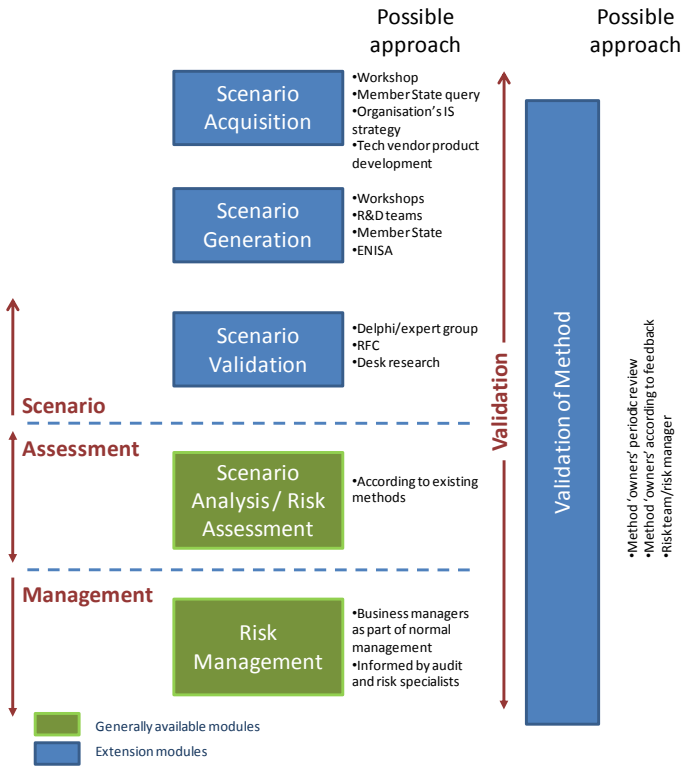

Figure 4: The missing modules

The generation and analysis of emerging and future risk scenarios within the developed module is structured though a formalised graphical notation. The notation provides elements to represent activities within the scenario, along with the entities that undertake these activities and the linkages and communications between activities. Each activity is then analysed for potential risks and the details of these risks are recorded on the scenario diagram. This facilitates exporting risk information into other risk assessment and management methods for further analysis, and provides a clearly defined interface to support this process.

Further work on this scenario-based approach resulted in the EFR Process Model that details the specific activities and tasks as well as the roles involved.

A high level overview of this approach is presented in the diagram below:

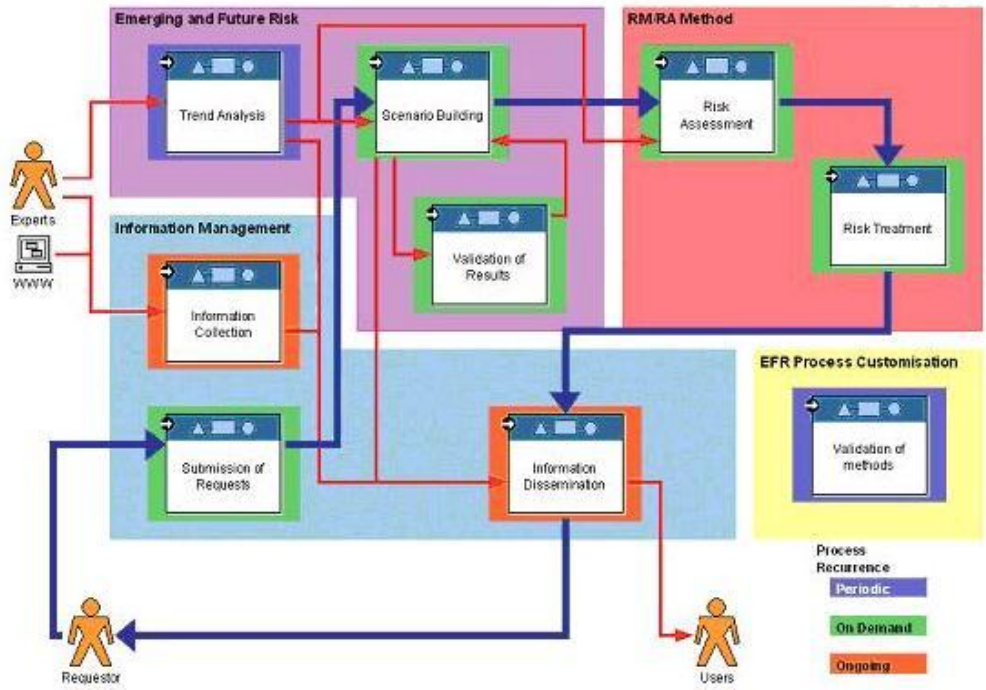

Figure 5: EFR Process Model

2. EFR Organisation and Implementation

The following chapter describes necessary aspects of the organisation and implementation of the EFR Framework.

There are a number of organisational and implementation aspects which require certain examination in order to execute the EFR Framework. Thus the following section outlines the involved roles and their corresponding responsibilities as well as various planning activities which should be considered.

The last part of the chapter deals with issues considering the implementation of the EFR Framework. Apart from a set of required conditions, a possible implementation form of the EFR Framework is also presented.

2.1. Organisational aspects

2.1.1. Roles and Responsibilities

The diagram below illustrates the organisational structure of the EFR Framework. This structure consists of personnel belonging to ENISA and includes further external parties which will participate in the EFR Framework.
The main part of this section deals with the ***Roles*** involved in the EFR Framework. Apart from possible skills the roles require, a description of each role with its assigned activities based on the RACI Model will be provided. The RACI Model lists the implied activities and defines the roles necessary to carry them out. Those **R**esponsible for actually doing the activity, those **A**ccountable for ensuring the activity is done, those **C**onsulted in the progress of the activity and those **I**nformed of the outcome.

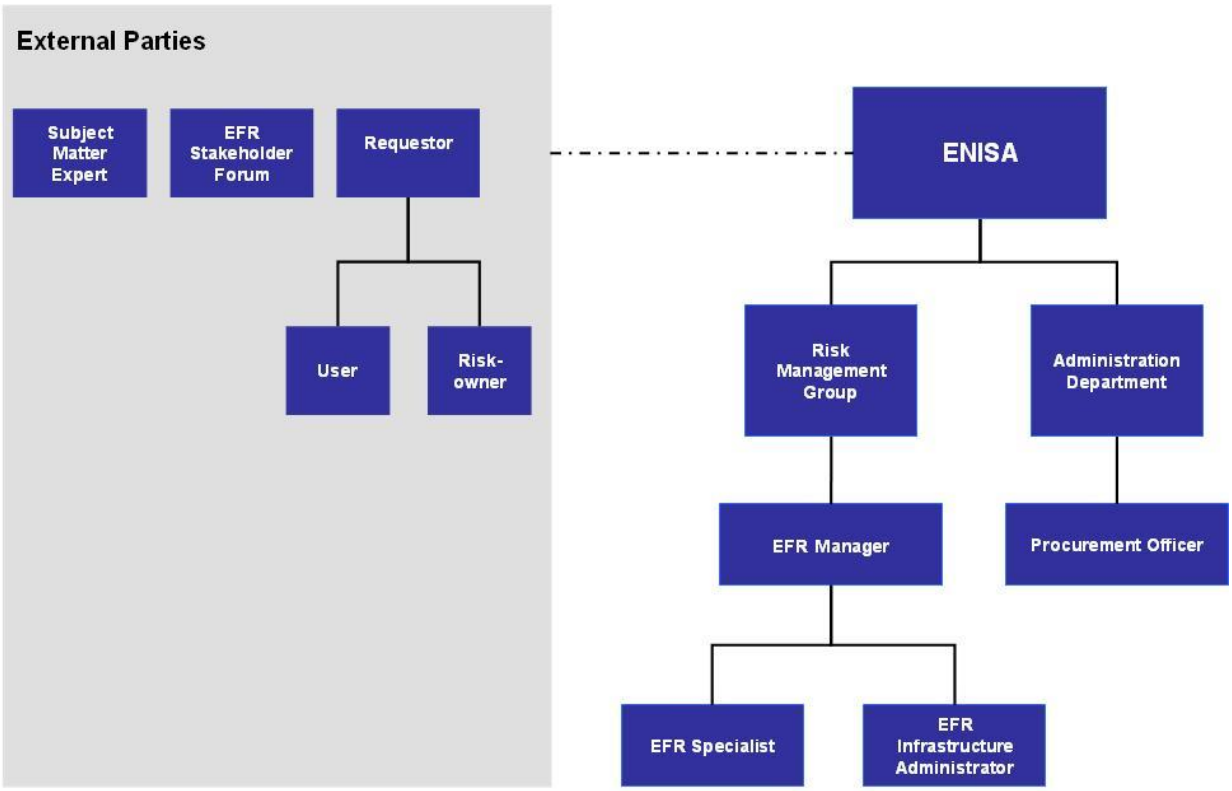

Figure 6: Organisation of the EFR Framework

1. User / Requestor

Any stakeholder (industry, academia, EU institutions, etc) may submit to ENISA ideas and proposals for topics (emerging technologies / applications) for identification of emerging and future risks utilising the EFR Framework.

However, ENISA may also receive a formal request for the identification and assessment of emerging and future risks which may only be submitted by:

- Member States considering the impact of new technology/applications and the need for introducing new or amendment policy
- The EC and other EU institutions considering the impact of strategic IS/IT planning or considering the development/implementation of new and innovative applications or technology

In this case, there is a separate process that would need to be followed internally in ENISA; therefore, we have identified this as a possibility in the development of the framework for completion purposes, and specified different steps that should be followed in this case.

It should be noted that the role of the "User" is not necessarily equivalent to that of the "Requestor". The "User" can also be any organisation interested in the outcome of the EFR Framework, i.e. a beneficiary of the results, even though this particular institution/organisation/entity has not submitted the request itself.

Following the **RACI Model,** the chart below illustrates the activities carried out by the requestor (in the case when a formal request has been made to ENISA) during the EFR Framework.

Responsible	Accountable	Consulted	Informed
Submit identity information	Define user's information requirements	Expert review of scenarios	Verify identity information
Submission of completed template		Review presentation of information	Redirect requestor to terms and conditions
Define user's information requirements			Formulate scenarios
			Select scenario template
			Accept scenarios
			Provide information to the target group
			Authenticate user
			Acquire information and present information to the user
			Redirect requestor to terms and conditions and the public website
			Acquire unclassified information
			Select and appoint experts

Table 7: RACI Model related to the User

It is noted that there are no specific skills required in order to participate as a user in the EFR Framework.

2. EFR Specialist

This role is primarily concerned with the risk related aspects of the EFR process. The EFR Specialist formulates a set of scenarios, identifies the context of information needs and classifies information in the system. This role is also accountable for all risk related information collection tasks and activities.

Following the **RACI Model,** the chart below illustrates the activities carried out by the EFR Specialist during the EFR Framework.

Responsible	Accountable	Consulted	Informed
Formulate scenarios	Identify actors	Not applicable	Acquire scenario from knowledge base
Select scenario template	Identify devices		Check technology
Analyse request	Determine activities to be undertaken		Check application
Identify context of information need	Populate scenario template		Acquire information on relevant new applications
Classify information	Expert review of scenarios		Acquire information on relevant existing or new applications
Identify skills required of experts for each scenario	Identify and capture sources of information		Acquire information on relevant new technologies
	Acquire information from each source		Acquire information on relevant existing new technologies
	Review of collected information		Extract information sources from K.B.
			Review presentation of information
			Index and formation information
			Review information indexing, formatting and storage

Responsible	Accountable	Consulted	Informed
			Select and appoint experts
			Extract information related to desired trend consideration
			Extract information on identified emerging and future risks
			Store information

Table 8: RACI Model related to the EFR Specialist

Possible required skills for this role are:

- Good interpersonal and communication skills
- Team player
- Ability to work under pressure
- Knowledge of IT environment
- Good analytical and planning skills

3. EFR Manager

The main task of the EFR Manager is supervising the actions of the EFR Specialist and EFR Infrastructure Administrator. This role is also accountable for the validation of the request and for the successful identification of the context of information needs and classification of risk related information. This role oversees the risk identification, analysis and assessment process to ensure its effective and successful operation. Moreover, this role is involved in the selection of experts from the pool of experts and gives access levels to the users registered in the authentication system. In addition to this, the EFR Manager is concerned with the information dissemination aspects of the EFR Framework, including the identification of target groups, support for the generation of information for these target groups and presentation of information to the users. The EFR Manager ensures also the smooth operation and quality of the entire process by reviewing and evaluating relevant aspects of the EFR Framework.

Following the **RACI Model,** the chart below illustrates the activities carried out by the EFR Manager.

Responsible	Accountable	Consulted	Informed
Identification of risks	Submit completed template	Identification of options	Analyse request

Responsible	Accountable	Consulted	Informed
Analysis of relevant risks	Formulate scenarios	Development of action plan	Identify and capture sources of information
Evaluation of risks	Select scenario template	Identification of risks	Acquire information from each source
	Analyse request	Analysis of relevant risks	Review of collected information
	Accept scenarios	Evaluation of risks	Review presentation of information
	Identify context of information need		Classify information
	Identify skills required of experts for each scenario		Review information indexing, formatting and storage
	Select and appoint experts		Select and appoint experts
	Identify risks		Expert review of identified EFR
	Analyse relevant risks		Identification of residual risks
	Evaluate of risks		
	Identify options		
	Develop action plan		
	Implement action plan		
	Identify residual risks		
	Approve action plan		

Table 9: RACI Model related to the EFR Manager

Possible required skills for this role are:

- Good interpersonal and communication skills
- Team player
- Ability to work under pressure
- Knowledge of IT environment
- Good analytical and planning skills

- Experience in team/staff leadership and motivation of being able to lead and motivate a team of staff
- Extensive knowledge of the EFR and Risk environment
- Knowledge of the maintenance activities of the EFR Framework

4. Subject Matter Expert

This role requires significant knowledge and experience in a certain subject area related to EFR identification and assessment which is usually determined based on the specific requirements of the submitted requests or the type of risks being identified or assessed. Among other tasks, the Subject Matter Expert will validate the set of scenarios, analyse trends previously identified and stored in the knowledge based management system, acquire information extracted by the knowledge based system to include areas covered by the formulated scenarios and review the collected information as well as the effectiveness of information collection methods to acquire the relevant and valid information. This role is typically recruited for particular assignments called in an ad-hoc basis. Thus, it is not a stable entity. The selection of the pool of experts will be done beforehand (see Procurement Officer).

Following the **RACI Model,** the chart below illustrates the activities carried out by the Subject Matter Expert.

Responsible	Accountable	Consulted	Informed
Select and appoint experts	Not applicable	Formulate Scenario	Select and appoint experts
Identify actors		Select scenario template	
Identify devices		Identify risks	
Determine activities undertaken		Analyse relevant risks	
Populate scenario template		Evaluate risks	
Expert review of scenarios		Identify options	
Identification and capture of sources information		Develop action plan	

Responsible	Accountable	Consulted	Informed
Acquire information from each source		Implement action plan	
Review of collected information		Implement action plan	
		Identify residual risks	
		Select and appoint experts	

Table 10: RACI Model related to the Subject Matter Expert

Possible required skills for this role are:

- Good interpersonal and communication skills
- Team player
- Ability to work under pressure
- Risk management knowledge
- IT knowledge
- Specific area knowledge related to the EFR

5. EFR Stakeholder Forum

The EFR Stakeholder Forum is a stable entity composed by ten experts. This role reviews and accepts the generated EFR scenarios and is consulted in the review of the collected information as well as in the methods to collect this information. The stakeholders are also consulted in the risk related tasks and activities and in the "Information Dissemination" before providing the information to the users. The Forum also ensures the smooth operation and quality of the entire process by reviewing and evaluating relevant aspects of the EFR Framework. The stakeholders may interact with the experts.

Following the **RACI Model,** the chart below illustrates the activities carried out by the EFR Stakeholder Forum.

Responsible	Accountable	Consulted	Informed
Acceptance of scenario	Not applicable	Review of collected information	Identification of residual Risks
		Review presentation of information	Select and appoint experts
		Select and appoint experts	

		Identify risks	
		Analyse relevant risks	
		Evaluate risks	

Table 11: RACI Model related to the EFR Stakeholder Forum

There are no specific skills the members of the EFR Stakeholder Forum need to fulfil in order to participate in the performance of the EFR Framework.

6. Risk Owner

The Risk Owner is usually the entity that is directly affected by the existence of risks. This role should identify possible risk treatment options, develop appropriate action plans, approve and implement action plans and evaluate residual risks. Similar to the EFR Manager, the Risk Owner is additionally consulted in the identification, analysis and evaluation of risks.

Following the **RACI Model,** the chart below illustrates the activities carried out by the Risk Owner.

Responsible	Accountable	Consulted	Informed
Identification of options	Not applicable	Identify of risks	Not applicable
Development of action plan		Analyse of relevant risks	
Approval of action plan		Evaluate risks	
Implementation of action plan			
Identification of residual risks			

Table 12: RACI Model related to the Risk Owner

There are no specific skills required in order to participate as a Risk Owner in the EFR Framework.

7. Procurement Officer

The Procurement Officer is responsible to assist the Risk Management Group in following a transparent and appropriate procedure for selecting subject matter experts. This is an internal role of ENISA and therefore, not related directly to the EFR Framework.
The selection of experts is done beforehand so that a pool of experts is available before starting the process. The final selection of candidates for a specific scenario is done by the EFR Manager.

Following the **RACI Model,** the chart below illustrates the activities carried out by the Procurement officer.

Responsible	Accountable	Consulted	Informed
Assist in selection of experts	Not applicable	Not applicable	Not applicable

Table 13: RACI Model related to the Procurement Officer

Possible required skills for this role are:

- Recognized HR Qualification
- Good interpersonal and communication skills
- Team player
- Ability to work effectively with EFR Manager at all levels
- Ability to work under pressure
- Knowledge of the EFR environment, in order to understand the core of the business and deliver an HR selection that supports the EFR Framework
- Good analytical and planning skills
- People Management skills

8. EFR Infrastructure Administrator

The EFR Infrastructure administrator undertakes all the activities and tasks required to ensure the continuous and correct operation of the systems that take part in the EFR Framework like the authentication and the knowledge-based management systems:

- *Authentication system*: This system is responsible for the identification of the Users (login and password) and the establishment of the appropriate access level granted to each User. Based on the relevant access level, the system will identify who can make requests and also the type of information they will receive from the EFR Framework
- *Knowledge based management system*: This system performs all the operations related to information storage, indexing, processing, retrieval and dissemination. This includes templates for requests submitted by users scenario templates, trend information, emerging and future risk information.

Following the **RACI Model,** the chart below illustrates the activities carried out by the EFR Infrastructure Administrator.

Responsible	Accountable	Consulted	Informed
Ensuring smooth operation of authentication system and knowledge base, maintenance	Verify identity information	Not applicable	Not applicable
	Redirect requestor to the terms and conditions		
	Authenticate User		
	Redirect user to the terms and conditions and the public website		
	Obtain template for submission of request from knowledgebase		
	Present user with a template for the submission of a request		
	Acquire scenario from knowledgebase		
	Export data to risk assessment method/tool		
	Check technology		
	Extract information related to desired trend consideration		
	Check application		
	Extract information on identified emerging and future risks		
	Storage Information		
	Index and formation information		
	Generate information for target group		
	Acquire information on relevant new applications		

Responsible	Accountable	Consulted	Informed
	Acquire information on relevant existing new applications		
	Acquire information on relevant new technologies		
	Acquire information on relevant existing or new technologies		
	Extract information sources from K.B.		

Table 14: RACI Model related to the EFR Infrastructure Administrator

Possible required skills for this role are:
- Good interpersonal and communication skills
- Team player
- Ability to work under pressure
- Good understanding of networking principles and practical application
- Knowledge in System administration
- General IT Knowledge
- Managing the Ticketing system, ensuring all incidences of this system and all teams of the EFR Framework to be dealt with.
- Technical Knowledge on how to maintain the EFR Framework

2.1.2. Planning

The planning part encompasses four subparts which will be described in more details in the following section.
- Time Scheduling,
- Budgeting,
- Working and meeting modalities
- Requirements on the selection and involvement of Subject Matter Experts

Time scheduling

Before starting to run the EFR Framework, the EFR infrastructure needs to be properly set up.The activities that will be carried out in order to appropriately develop the required EFR infrastructure are the following:

1) Setting up the development environment

This task will set up the complete run-time environment of the platform to proceed with the implementation of the EFR Framework.

- Installation and configuration of the server
- Installation of the platform on the server: This step will install the minimal set of components or features of the appropriate platform to implement the EFR framework
- Configuration of the platform

An important factor is the selected mode of deployment (in house or externally hosted platform used in "software as a service" model):

- In the "in house mode", the platform would be installed at ENISA office in Heraklion so it is important to know which kind of support the platform owner would provide in this location. Besides these current components, it is further significant to appraise the global picture on WF market and the future of the company that owns the product (the selected platform might disappear or could be bought by another company). Another issue to be considered when choosing the in house platform is the existence and cost of a trial license.
- A completely different set of selection criteria might be applied if the selected mode is an outsourced (hosted) platform and the software functionalities are provided following the "software as a service" model. ENISA would pay for active users (about 20 euros user/month) of the EFR platform. This approach involves a virtually risk-free deployment, especially since the EFR platform is still evolving.

A commercial trial license has the following advantages and disadvantages:

1. Depending on the tool and license, it is likely to include commercial tools for document management and workflow engine, while in SaaS mode these could be separated services
2. Initial cost is close to zero, although, if selected, there is a need to pay a commercial license later. This might be expensive (study shows that it pays off only after 5 years of running the platform in-house after which a new version or new technology might be considered).
3. There is a maintenance cost, need to estimate administrator allocation (related to a number of users, processes to be implemented or modified and instances to be managed e.g. for statistical purposes)

A cheap or open source license changes the picture slightly, since here the main cost category is maintenance. Solutions based on this selection are more unpredictable since there are no guarantees (e.g. in terms of high-grade security) and, at the moment it is only recommendable for non-critical parts of the EFR the process.

An external hosting facility with administrator services can be calculated as a flat fee, per process instance (more common in pure Workflow platforms), per project or per user (more common in collaboration oriented platforms). Advantages include scalability (processes and users can be easily added), administrator services 24x7, and, depending on the contract, even complete maintenance, normally in cases where the provider of the hosting is also the workflow developer. It can become expensive if the number of users and running process instances grows exponentially. One disadvantage is the relative dependency on the hosting provider, which becomes high if it includes complete maintenance (same company develops, implements, processes and hosts the platform).

2) Implementation of the EFR Framework

The different parts (roles, activities, data transferred between the activities) of the EFR Framework will be developed on the platform.

3) Assessment and validation of the EFR Framework on the platform

The main purposes of the testing are:

- The validation of the EFR infrastructure and the requirements
- Testing the workflow
- Assessing the practical usability and usefulness of the application provided
- The collection of information on performances and usability provided by possible users of the platform
- Collecting suggestions for improving the EFR infrastructure as a whole
- Identifying the points of strengths and weaknesses of the application.

The evaluation of the EFR infrastructure should include the following criteria: usability, reliability, effectiveness, conformance with the initial requirements and specifications and also user acceptance and satisfaction.
Therefore, for the evaluation phase, these steps will be followed:

- Checking the conformance with the requirements and specifications
- **Usability**: Labelling the EFR infrastructure as usable means that the infrastructure is sufficiently documented and structured that it can be used by someone with an average knowledge of the interface and the domain to be addressed.
- **Reliability**: The EFR infrastructure will be reliable if it runs properly and consistently.
- **Cost-effectiveness**: The EFR infrastructure can be considered as cost-effective when it provides the expected services with a reasonable effort in time and consumption of other resources
- **User acceptance and satisfaction**: Attaining user acceptance and satisfaction will be the final goal for the EFR infrastructure. User acceptance and satisfaction is more than the sum of all the previous validation processes. However, a good perception on reliability, usefulness, efficiency and conformance is a pre-requisite for user acceptance and satisfaction; nevertheless it is not a condition.

4) Maintenance of the EFR Framework
Keeping the EFR Framework current and updated is a key factor in order to maintain its relevance and usefulness. Therefore, a maintenance plan has been set up to support ENISA as a useful tool when scheduling the important tasks of keeping the EFR Framework updated in the future. The maintenance will be an on-going activity during the whole life of the EFR Framework. A detailed description of the maintenance plan will be elaborated in the last chapter of this handbook.

5) ***Performance of the EFR Framework*** from the identification of a topic for a scenario until the dissemination of the information. This activity is further described below.

The relationship between the different activities is represented in the following figure:

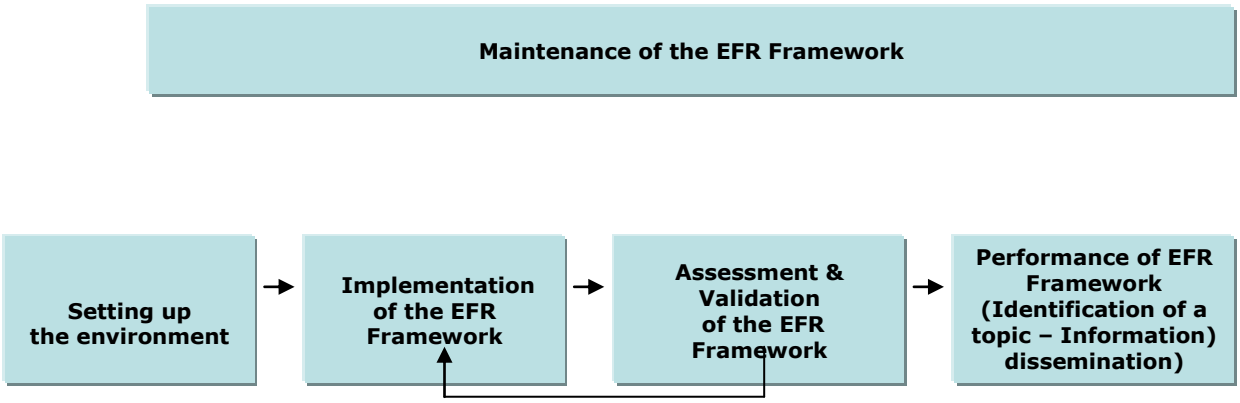

Figure 15*:* Relationship between all activities of the EFR Framework

The following Gantt chart shows the timing of the activities establishing the EFR infrastructure

Week	1	2	3	4	5	6
Setting up development environement						
Implementation of the EFR Framework						
Assessment and validation of the platform						
Maintenance of the EFR Framework	Ongoing					

Figure 16: Timing of the activities establishing the EFR infrastructure

Once the EFR Framework is properly installed and functioning, its actual performance can start. A time scale of three/four months in order to run the EFR Framework from the identification of topic for scenario until the dissemination of the information has to be assumed.
Further the EFR activities were classified taking into account activities which are carried out "on demand", "on a periodical basis" and activities which are continuously being performed ("on going").
The Gantt chart below illustrates the different activities of the EFR Framework in a time frame of 14 weeks. It has been assumed that the Trend Analysis would periodically be carried out in order to provide the EFR Framework with actual information. Subsequently the following activities are presented according to the time those require in order to be performed. Please note, in case the scenario has not been validated and needs further refinement, one week to carry out this task has been assumed before the analysis can take place.

Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Trend Anaysis					Periodical									
Submit and validate a request														
Scenario building														
Validation of scenario description														
Scenario refinement														
Scenario analysis														
Risk assessment														
Risk treatment														
Information collection					Ongoing									
Information dissemination					Ongoing									

Figure 17: Timing of EFR Framework activities

Budgeting

The budget of the EFR Framework will mainly depend on the implementation mode that will be chosen. As described in one of the next chapters, the platform on which the EFR Framework will be implemented could be set up according to two different operational modes, the "in house mode" and the "external hosting". Therefore, different issues of each mode need to be taken into consideration when establishing the budget

In House mode

The EFR Infrastructure (platform & support services) is sold as a product to ENISA and it is installed through integration into the ENISA's existing technological infrastructure. At the same time, ENISA obtains software changes and improvements paying an annual maintenance fee. In addition, the party will provide optional consulting and training services.

The Direct Sale will be accomplished via the sale of:

- Platform Licence: Licenses allow the use of the software for a period of time
- Support Services: Basic Maintenance Services, Advanced Maintenance Services, Training & Consulting Services.

In the in house mode, ENISA would pay a package of product (system software) & supporting services.

The costs in this scenario could be composed by the following elements:

- **Software Licence fee**: This fee is the cost of the software ownership for ENISA. The licence fee may be determined on an annual basis, however, and upfront payment is also made, which is an initial fee linked to installation and the basic customisation of the software. These services will comprehend costs for the installation/customisation of the software.

- **Maintenance cost**: it represents the cost for the platform maintenance, server administration, internet costs and the cost of the personnel.
- **Support service fee**: Fees for optional services such as training, consultancy and further development services will be determined on the basis of man-days required on a "project" basis.

External hosting/Software as a service (SaaS):

The SaaS hosting is one model to deploy external hosting. In the SaaS hosting Scenario, a third party will host the EFR platform in a server within its own infrastructure and will operate software applications on behalf of ENISA

The SaaS model will rely on "Basic Hosting" model. Basic Hosting means that applications will run on the party SaaS infrastructure, and it will be delivered to clients via the Internet. The party will remotely host and deliver a packaged application to ENISA from an off-site, centralized location. ENISA does not have ownership of the application but instead "rents" the application, typically on per user basis.

The costs in this scenario could be composed by the following elements:

- **Usage fee:** In this case ENISA rents the application on per user basis or at a flat monthly rate or a flat annual rate including the rent of a space on the sharing server, which remains property of the provider.
- **Support Service fee**: fees for optional services such as training and consultancy services.

Additional costs to be taken into consideration are the fees and expenses of the experts as well as the organisation of the conferences and meetings related to the EFR Framework (e.g. meetings for experts to discuss a scenario).

Working and Meeting Modalities

Meetings can be very productive, if they are underpinned by appropriate meeting modalities. Therefore, the implementation of a good and efficient meeting structure between the different actors of the EFR Framework is essential. Apart from the general and basic planning elements which encompass a good meeting (set agenda, list items of review, identification of responsible person to speak, follow-up plan, etc.), the best working and meeting modalities to use throughout the EFR Framework should be determined and implemented.

First of all, a transparent working structure should be followed during the process. It is important to have transparency regarding results, progresses and processes. Ensuring all actors with the same level of knowledge will be important.

The actors of the external organisations working together with ENISA, and the actors of the Risk Management Group and Administration Department belonging to the structure of ENISA, probably develop particular ways of interacting with each other over time. Effective interpersonal communication among members of the same group and successful communication with managers and employees external to the team are critical components of team functioning.

The different functions that the involved actors fulfil might as well implicate diverse working and meeting modalities which have to be developed. Since holding a central role within the EFR Framework, the EFR Manager needs to interact more frequently with other roles than for instance the EFR Infrastructure Administrator. In accordance with his supervising tasks, he needs regularly to be informed and updated about the results or incidences produced. Therefore, periodic meetings and efficiently established communication channels with e.g. the EFR Specialist, the EFR Infrastructure Administrator or the Procurement officer should optimize the EFR Framework. These face to face meetings can be supported by regular reports, which could be submitted in specifically designed templates. Efficiently established communication channels between e.g. the EFR Manager and the other implied roles are essential to cope with his central position. In general terms, efficiently organised communication channels are a basic constraint in terms of working and meeting modalities.

Within the EFR Framework the Procurement Officer assists the EFR Manager and the Risk Management Group selecting appropriate subject matter experts. This requires, for instance, the organisation of meetings with the candidates as well as with the actors responsible for choosing the experts.

Face to face meetings are preferred, since it is apparently the best way to transmit and discuss a certain topic. This working modality adds a lot of operational understanding of the various roles and responsibilities of the EFR Framework. A weekly general meeting for all the employees working in the EFR Framework should be held in order to review progress, to obtain broad input, and to coordinate shared work processes. These meetings are complemented by basic working modalities such as email, phone calls, written reports and a ticketing system.

Besides physical meetings, the implementation of a ticketing system can be useful, thus everyone who has a request to another employee concerning information search, problem solving or incidents can post them in the system. This kind of working modality eases the follow up and management of the requests.

By this mean the EFR Manager could, for example, report all incidences related to the authentication system and the knowledge base management system to the EFR Infrastructure Administrator and vice versa.

Working and meeting modalities external to ENISA

Apart from this, the interaction with external parties in terms of working and meeting modalities needs also to be considered in order to support the proper functioning of the EFR Framework.

ENISA works together with different external parties:

- **Subject Matter Experts**: face to face meetings will take place once or twice during the 3-4 month scenario. Supposing that these physical meetings are not sufficient, and for instance a refinement of a scenario set up is required, other modalities will be taken into account. Here it would be convenient to adopt frequent video conferencing systems/teleconferences as much as possible.
- **EFR Stakeholder Forum**: face to face meetings with the EFR Forum will only take place two or three times a year

In both cases the meeting place would be Athens or Brussels.

Requirements on the selection & involvement of Subject Matter Experts

The Subject Matter Experts function as an ad hoc workforce, i.e. they are established for a specific purpose. This is a very efficient way of working, although the availability of these experts during the whole EFR Process has to be assured. When involving the experts, ENISA needs to be able to rely on the performance of these resources without failure.

An initial panel of experts appointed by ENISA will be constituted beforehand. ENISA shall draw up the list of experts on the basis of the results of an open call for expression of interest to be widely disseminated through the web site of the Agency and elsewhere deemed appropriated. The call shall invite experts from many disciplines as for example cryptography, biometrics, risk analysis and management, network and information security, and electronic processes etc. These disciplines should be represented by different types of stakeholders such as the information and communication technology industries, academic institutions or consumer organisations etc that express interest and willingness to participate in the work of the group. The Procurement Officer assists the Risk Management Group in following a transparent and appropriate procedure for selecting the experts.

The selection is based on the following criteria:

- Demonstrated expertise and experience in the scenario's field considering the academic record in terms of published papers and studies on the required skills, as well as expertise and technological knowledge in the required field;
- Fair representation of relevant stakeholders (industries, academic, consumer organisations etc.): It could be constructive to combine different experts in the same scenarios, so we are able to contrast opinions and exchange knowledge between the experts, in this way the best information possible will be obtained. This expert knowledge sharing will encourage advantages in terms of new discoveries and innovation. This will also result in more trust between different experts.
- Gender balance
- A balanced geographic distribution in terms of nationalities of the involved experts could be a minor consideration

2.2. Implementation aspects

2.1.1. Required IT Components

In order to deploy the EFR framework, an **appropriate platform** is expected to be identified and deployed. The platform, which is yet to be implemented, will need to address the following requirements:

- *Concurrent use*: Several users should be able to access to the platform at the same time.
- *Collaborative platform*: The EFR Framework requires collaboration between the different roles involved (e.g. Subject Matter Experts and EFR Manager). Thus, the platform should allow the capture, sharing and retrieval of information across teams. Teams should be able to rapidly find relevant content, experts, look at past or similar scenarios and keep on top of any relevant changes to make them more efficient.
- *Document management* to deal with lots of different documents, like requests, scenario templates, risk assessment documents. Desired features are:
  - *Multiple formats* (Word, PDF,..).
  - *Check in / Check out*: Check out will prevent users from writing at the same time: This feature will be very useful when two or more subject experts work in the same scenario at the same time
  - *Version control*: Changes to these documents are usually identified by incrementing an associated number or letter code, termed the "revision number", "revision level", or simply "revision" and associated historically with the person making the change.
- *Web connectivity* to allow users to connect to the platform via the Internet. This feature will allow requestors to make their requests remotely through the web. Moreover, subject matter experts may analyse scenarios via web.
- *Notification*: The platform should offer a centralized means of sending messages to users via a variety of channels such as email, IM, SMS, etc.
- *Access control*: An Access Control that contains the information about the permission and how it relates to an authority. This feature will serve to control the users that are allowed to make requests or people who are authorised to, for example, retrieve a template scenario.
- *Workflow*: The platform should allow the execution of a large number of steps. Required workflow features are:
  - Enter workflow parameters (priority, due date),
  - Attach resources to workflow (i.e. scenario documents),
  - Assign workflow participants
  - List tasks assigned to user, completed by user, assigned to the user's pool
  - View & Manage Tasks: edit task related information, add commentaries, review workflow history, view and perform operations (checkout, edit, delete) on attached documents, attach new documents to workflow, re-assign task to another user, mark task as done, take ownership or return to pool
  - Cancel workflow
  - Simple review & approve workflow
  - Simple ad hoc task workflow

Different **operational modes** for the platform will be also studied:

- In house mode: Platform would be installed at the ENISA office in Heraklion
- External hosting: Platform will be outsourced and the software functionalities are provided following the "software as a service" (SaaS) model

We compare the SaaS model with the traditional approach in which a software vendor sells the software license and the customer runs the software on its own technology infrastructure. This analysis emphasizes the features of the SaaS model that can help ENISA to solve their IS/ICT problems in new and more efficient ways then the traditional approach.

Differentiator	SW as a Service (SaaS)	Traditional Approach (SW as a License)
Main characteristics	SaaS controls all necessary ICT resources and delivers application functionality to a large number of customers as a service via Internet. Many users from different organizations at a time use the same application.	Software vendor develops the application; the application is implemented on customer's HW and customer is responsible for the operations.
Design and Technology Issues		
Design premise	Designed from the outset for delivery as Internet-based service for a large number of customers. It includes specific HW and SW architectures, and business model.	Designed for implementation and customization by specialist and for customer to operate and maintain.
Technological architecture	Multi-tenant service oriented architecture designed to run hundreds or thousands of users from different user organizations on a scalable technological infrastructure.	Architecture suitable for deployment by individual company on a dedicated ICT infrastructure.
Client interface	Browser is the main and often the only interface for all applications. It eliminates the need to develop, install, and support multiple client interfaces.	Many SW vendors have added browser interfaces, but most support multiple clients – it increases development, installation and support costs.

Service management	Applications with embedded service management, monitoring metering and security capabilities.	Typically must add service management, monitoring and metering features subsequent to product development.
Upgrades	Frequent (every 3-6 month) upgrades possible. Provider is responsible for upgrade. All customers are upgraded simultaneously resulting in significant cost reductions.	Infrequent, major updates (every 12-24 months). Individual customers may be running different versions of software. Both, provider and customer, have to implement version management process.
Business Issues		
Readiness of the service	Short implementation cycle. Typically no requirements for new HW and SW	Long implementation cycle due to complex implementation of HW, SW, and knowledge transfer to customer sites.
Availability of the service	The service is available any time (365x24) and from any location (globally).	Could be limited to single organization via intranet or client/server interface.
Scalability of the service	The volume of the services delivered (i.e. number of users supported, number of transactions) can be scaled (up or down).	Configuration needs to support peak requirements, and cannot be scaled down.
SW licenses	ENISA does not buy SW licenses. The charge for SW usage is included in the service price.	It is necessary for ENISA to buy a SW license. The flexible changes of SW licenses number is rather difficult.
Reliability of the service	Typically very high. Provider can more efficiently invest in network and systems redundancy. If he does not assure high reliability he loses customers' business.	It is very expensive to provision true fault-tolerance for in-house applications. Most companies remain at risk and typically experience periodic downtime.
Flexibility to business changes	Good if alternative service providers are available. Direct provider – user contact can shorten the time of new requirements implementation.	Good if the business change requires only minor application changes. Inflexible if the business change requires major application changes or new application development.
Customisation	Typically limited.	Extensive customisation possible (at both configuration and source-code levels), but expensive.

Functionality	Often limited functionality, application typically designed for narrow vertical market.	Extensive functionality, customers often use only small part of the available functions.
Evaluation of an application by user	The application can be evaluated before the purchase.	Application is evaluated after purchase, installation and customisation.
Internal sources utilization (people, technology, etc.)	Only few internal sources used for ICT processes support. Most of the company sources can be used for core business processes.	Many internal sources used for ICT processes support.
Costs of ICT	Predictable, no investments required -operating costs only. The costs are highly correlated with the volume of services. SaaS pricing usually includes a one-time license-and-setup fee that's significantly lower than a standard software licensing fee and a recurring subscription fee that covers hosting and maintenance.	Both investments and operating costs. High overhead costs given by depreciation and amortizing of investments. The costs may not correlate with the volume of service delivered.
ICT Management Issues		
Subject matter of the contract	The Service Level Agreement (SLA) constitutes the main part of the contract. SLA defines: content of the service (functionality, data, training, support,...), volume (number of users, number of transactions, volume of data,…), quality (availability, response time, security,…) and price.	Usually, the contract divided into several subcontracts for hardware, SW licence, service (implementation, integration, training, upgrade,…).
SLA	The usage of SLA is a standard requirement	SLA in most cases not used.
Responsibility for ICT infrastructure	Provider.	Customer (but some of the activities often realized by third parties).
ICT sources utilization	ICT sources of the provider (HW, SW, ICT specialists) are used across all customers; provider has advantages of	ICT sources are used only for one organization.

	economies of scale. Customer ICT sources are minimized.	
ICT knowledge required at customer site	How to use ICT for competitiveness enhancement, available services at ICT market, SLA structure, and management of service delivery.	The same as in SAAS plus: wide spectrum of ICT knowledge. The required ICT knowledge is dependent on number of platforms and types of application used. Extensive technical training needed
Size of ICT personnel at customer site	Very small.	Large – different types of specialists needed.
Problem and change management procedures	Short feedback cycle - procedures enable almost immediate feedback. Support staff or programmers can directly identify and fix problems. Fixing a problem for one customer fixes it for everyone, which reduces support costs.	Problem solving is often indirect via intermediaries (VARs, SIs, etc). Patches and upgrades are implemented at individual customer sites. Costly and unreliable, as customers often delay installation of patches and upgrades.
Main risks	Loss of expertise that could be useful in the future. Stability of the provider (Exit strategy). Unsatisfactory customisation. Unresolved systems integration issues – who should be responsible for integration? Enhancements not under control of the customer. Security. Satisfactory response time.	Stability of the provider – but not to the same extent as for SaaS. Technology backwardness. High TCO (Total Cost of Ownership). Low flexibility and scalability.

Table 18: Comparison of the software-as-license vs. software-as-a-service models for enterprise applications

The above table includes a number of compelling arguments that will make the software-as-service model a preferred solution for the development of the EFR Framework platform.

2.2.2. Non Disclosure Agreements

A Non-Disclosure Agreement (NDA), also known as a confidentiality agreement, Confidential Disclosure Agreement (CDA), Proprietary Information agreement (PIA), or secrecy agreement, is a legal contract between at least two parties that outlines

confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to.

It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information. As such, an NDA protects non-public business information.

NDAs are commonly signed when two companies or individuals are considering doing business and need to understand the processes used in each others business for the purpose of evaluating the potential business relationship. NDAs can be "mutual", meaning both parties are restricted in their use of the materials provided, or they can restrict the use of material by a single party.

- In the EFR Framework the NDA should/could be established between ENISA and the *Subject Matter Experts* through which the Subject Matter Experts agree not to disclose information covered by the agreement. The Subject Matter Experts, even after their duties have ceased, are subject to the requirements of confidentiality. In particular, they shall be required not to disclose information of the kind covered by the obligation of professional secrecy, such as information about undertakings, their business relations or their cost components, as well as information related to the investigation of criminal offences and the application of criminal law.

- In the EFR Framework the NDA could also be established between ENISA and the *Requestor* through which ENISA agrees not to disclose information related to the requests and the risk assessment results, even after their duties have ceased they maintain subject to the requirements of confidentiality. In particular, they shall be required not to disclose information of the kind covered by the obligation of professional secrecy, such as information about undertakings, their business relations or their cost components, as well as information related to the investigation of criminal offenses and the application of criminal

- As was mentioned before two different modes of deployment may be selected: in house or externally hosted platform following the "software as a service" model. If the selected mode is the second one, an additional NDA among ENISA and the *EFR platform service provider* has to be signed through which the organisation that provides the service agrees not to divulge any "EFR Framework" confidential information to any of its affiliates, subsidiaries, business partners or any other entities. In the event that ENISA or the party decides to withdraw from the contract, the party should agree to destroy all information provided by ENISA relating to the EFR Framework, but will still be bound by the confidentiality clauses.

2.1.3. Service Level Agreements

A Service Level Agreement (the Agreement) is an agreement between two parties for the delivery of specified services. It is effectively a proxy contract in which the two parties

have negotiated and signed a comprehensive document specifying the terms and conditions under which the service delivery may be effected.

In the context of the EFR Framework, there is the possibility to establish a *SLA between ENISA and the Subject Matter Experts*. Both parties must clearly understand their respective roles and responsibilities in respect of the delivery of the services and this information should be included in the Agreement.
The possible SLAs defined between ENISA and the Subject Matter Experts will contain at least the following features.

- Definition of the Service to be delivered by the Subject Matter Experts
- Terms and basis under which the Service will be delivered
- How the Service performance levels are to be measured
- Legal framework for the relationship between ENISA and the Subject Matter Experts
- Financial aspects of Service delivery including fees, expenses and penalties.

Depending on the type of scenario selected (in house, SaaS), different SLAs should be signed between ENISA and the EFR platform service provider.

- If the mode of deployment is *in house*, SLA in most cases is not used. Usually, the contract is divided into several subcontracts for hardware, SW licence, service (implementation, integration, training, upgrade,…).

- If the *SaaS* model is selected, the usage of SLA is a standard requirement. Thus, the SLA constitutes the main part of the contract. An approximate content of the SLA would be:
  1. Introduction
     - 1.1. Purpose and objectives
     - 1.2. Parties to the Agreement
     - 1.3. Commencement date
     - 1.4. Duration of the Agreement
     - 1.5. Definitions
  2. Scope of Work
     - 2.1. Standard Service
     - 2.2. Content of the Service (functionality, data, training, support,…)
     - 2.3. Volume of the Service (number of users, number of transactions, volume of data,…)
     - 2.4. Quality of the Service (availability, response time, security,…)
     - 2.5. Place of Service Delivery
     - 2.6. Changes of Service
  3. Performance, Tracking & Reporting
     - 3.1. Key personnel changes
     - 3.2. How the service will be monitored
     - 3.3. Benchmarks, targets and metrics to be utilized
     - 3.4. Service Level Reporting
     - 3.5. Service Review Meetings
  4. Problem Management
     - 4.1. Support and service desk services

4.2. Problem definition
4.3. Problem escalation
5. Compensation
5.1. Professional fees
5.2. Reimbursable expenses
5.3. Invoices
5.4. Payment terms
5.5. Taxes
5.6. Interest for late payment
6. ENISA's Duties and Responsibilities
6.1. Processing and authorisation of invoices
6.2. Training on special equipment or tasks
6.3. Approvals and information
7. Warranties and Remedies
7.1. Quality Of Service
7.2. Indemnification
7.3. Third party claims
7.4. Exclusions
7.5 Remedies for breaches
7.6. Force Majeure

3. EFR Framework

The **EFR Framework** is a scenario-based model which has been developed in order to assess Emerging and Future Risks. The model consists of a set of activities to be carried out while performing the EFR Framework. The following chapter analyses these activities including the description of the involved roles and their corresponding responsibilities as well as the information flow that each stage of the model entails.

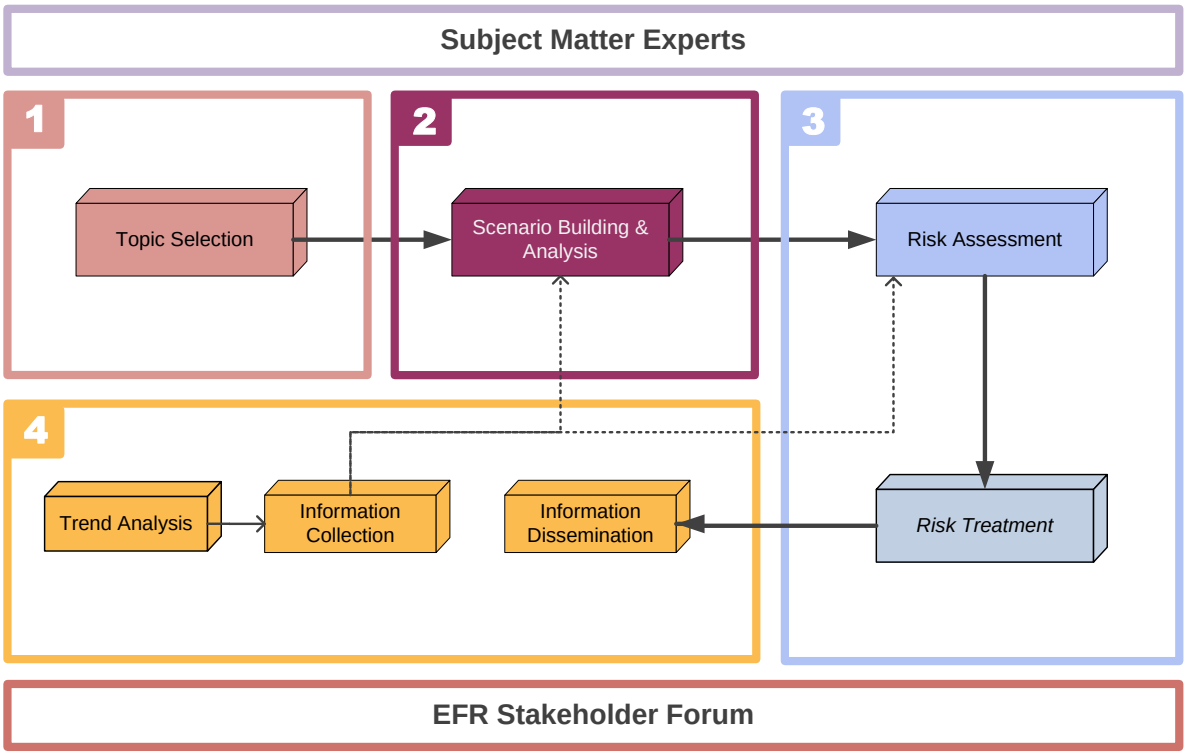

Figure 19: High level overview of the EFR Framework

The diagram above presents a high level overview of the EFR Framework.

In the following section each phase of the EFR Framework will be described in more detail. This includes the involved roles and the main activities that are carried out during the phase.

3.1. EFR Topic Selection

In the beginning, the topic, namely the particular technology and / or application to be assessed, is selected, based on proposals received from our stakeholders (industry, academia, Member States, EU Institutions). After the initial identification of the topic, the scope will need to be defined, as well as which areas to target in the possible scenario (especially if the topic, technology selected is too broad).

As mentioned in section 1 of this document, the topic, i.e. the particular technology / application to be assessed for emerging and future risks, may be also formally requested by:

a) Member States considering the impact of new technology/applications and the need for introducing new or amended policy

b) The EC and other EU Institutions considering the impact of strategic IS/IT planning or considering the development/implementation of new and innovative applications or technology.

3.2. Scenario Building and Analysis

Based on the selection of the topic and the scope identified, as well as the requestor's particular requirements (in case of a formal request submitted to ENISA), a specific scenario is formulated.

The expertise of members of the EFR Stakeholder Forum supported by the knowledge of the Subject Matter Expert and the results of the Trend Analysis (see paragraph 3.4.2) will form an essential part in generating relevant and validated scenarios. The generated scenarios are stored in the knowledge base for future reference and evaluation.

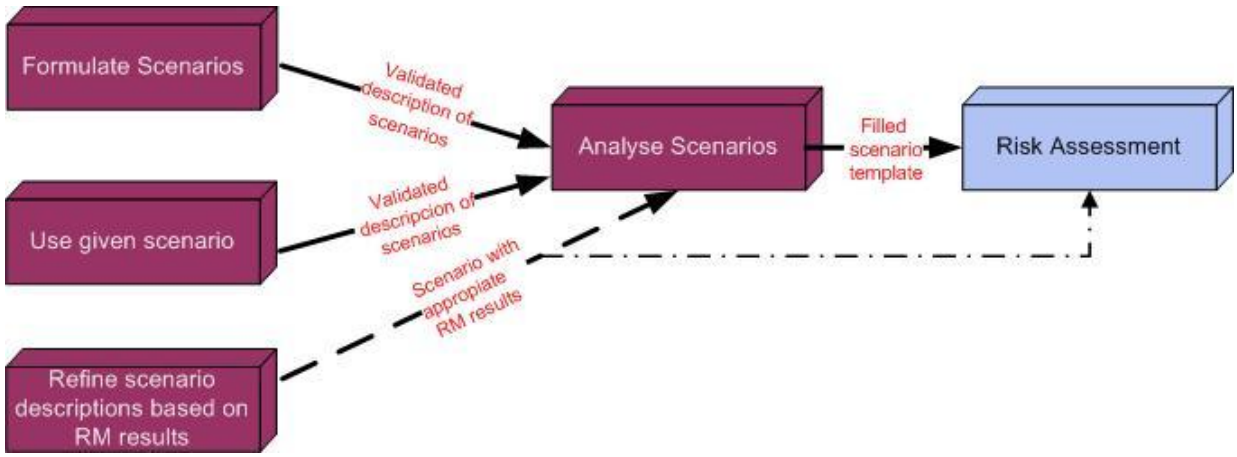

Figure 21: Scenario Building and Analysis

1. Scenario building

The scenario would either have to be built from the beginning or could be provided by the requestor. In the former case, the scenario would need to be formulated using several information sources. These sources could be current trend reports (Trend Analysis), the user-specific request template websites, research papers, white papers treating with the topic of the scenario to be built.

Considering this input, the EFR Specialist will construct a scenario relevant to the submitted request. Additionally, the Subject Matter Expert and the EFR Manager will provide guidance on this matter.

Input of this activity:
- Validated scenario
- Scenario template
- RM results

Output of this activity:
- Filled scenario template
- Scenario with the appropriate RM results

Once a first approach of the scenario is produced, it will need to be properly reviewed and validated. It should be noted that this is an iterative process and may require many iterations between actors. *More information on this procedure can be found in Validation of scenario description, Annex I.*

Use given scenario:
In case the requestor provides a specific scenario, this may be used as is. The description of the given scenario will then need to be reviewed by the EFR Manager and the expert before it can be validated.

2. Scenario analysis:

After a stable and validated version of the scenario is reached, the knowledge base is consulted in order to verify if a template with the required features already exists.
If there is no corresponding data in the knowledge base, the scenarios need to be analysed by the EFR Specialist in cooperation with the Subject Matter Expert. They are the ones who define the content the final scenario template should have.

At this point the scenario template will be completed. The obtained data of the validated and properly structured scenarios represented in the filled out scenario templates are hereafter fed into to Risk Assessment in order to identify the threats, vulnerabilities and impacts relevant to each scenario and the implicated potential risks. You can find an example of a scenario template in Annex III-Template.

If necessary, the scenario with the corresponding scenario template could be refined after the first level Risk Assessment has been made. This would represent a feedback situation as the results from the Risk Assessment/Risk Treatment phase are added to the scenario description. By doing so, we would receive a description of a set of scenarios including the already defined Risk Management results. As a last step, there needs to be decided if this

refined scenario requires a new analysis by the corresponding experts before transferring the altered scenario description once again to the *Risk Assessment*.

(More information on the input and output of this activity can be found in Annex II - Related input and output of activities)

3.3. Risk Management

The Risk Management as an activity carried out during the EFR Framework, consists of two subsequent stages: the Risk Assessment and the Risk Treatment, which is optional.
At this point it should be stressed out that any risk assessment method can be employed. As an example you can find a selection of RM/RA Methods on the ENISA website: http://www.enisa.europa.eu/rmra/rm_ra_methods.html

3.3.1. Risk Assessment

The primary purpose of the scenario generation process is to create valid scenarios to facilitate the assessment of emerging and future risks. The risk assessment process utilises the generated scenarios to identify relevant assets, threats and vulnerabilities relevant to each scenario in order to analyse potential risks.

Every organisation is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfilment of its objectives. **Identification**, **analysis** and **evaluation** of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. Appropriate **risk treatment decisions** are then produced based on the evaluation of these risks.

It has to be noted, that Risk Assessment is a process that in many cases is not (at least not adequately) performed, even if Risk Management is implemented. It is one of the main objectives of ENISA to generate awareness of this fact, but also to facilitate the use of Risk Assessments by providing practical examples.

Throughout the performance of the entire Risk Assessment activity the EFR Manager is the key actor involved. While undertaking the assessment of risks he will also consult the Subject Matter Experts, the EFR Manager and the Risk Owner.

There are a set of input and output data transmitted and generated while identifying, analysing and evaluating of risk. You can find the complete input/output list of RA and RT in the Annex IV **-** Input/output RA/RT.

Identifying risks
High quality information and a thorough knowledge of the organisation and its internal and external environment are very important while identifying risks. This process needs to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is essential that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organisation.

Analysing risks
Risk analysis is the phase where the level of the risk and its nature are assessed and understood. This information is the first input to decision makers on whether risks need to be treated or not and what is the most appropriate and cost-effective risk treatment methodology.
In general terms risk analysis involves: examination of risk sources, their positive and negative consequences, the likelihood that those consequences may occur and the factors that affect them, assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks.

Evaluating risks
At this point the EFR Manager evaluates for example the controls, impacts and threats relative to assets which could be produced in the specific scenario.
Considering this input, a risk treatment decision might needs to be elaborated. This means that it has to be decided which risks require treatment and which do not, as well as how the treatment priorities should be arranged. This decision could be based on the fact that the evaluated risks are relevant and therefore will imply threats to assets of the involved organisation.
Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the Risk Management context (i.e. in the risk criteria identification stage). These decisions require the collaboration of the Risk Owner and the Subject Matter Expert in order to choose which Risk Treatment should be deployed.
It is important to note that in some cases the risk evaluation may lead to the decision that further study needs to be undertaken, which implies that the assessment will start again with the analysis of risks.

3.3.2. Risk Treatment

In the context of the EFR Framework, Risk Treatment is optional, in the sense that the activities might stop at the identification of risks, depending also on the requestor's specifications.
According to its definition, Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. While the Risk Assessment has produced appropriate risk treatment decisions, this process is focused on the implementation of these decisions to mitigate the impact of these risks.
Possible options for Risk Treatment are identified based on the risk treatment decision, and an action plan is developed that contains specific actions to counter the risks. The action plan should be approved by the Risk Owner before it is implemented. It is important to identify and evaluate the risks that remain after the implementation of the action plan (residual risks) and a decision should be made on whether or not these risks need further analysis.

Identification of options
Having identified and evaluated the risks and decided to carry out a risk treatment, the purpose of this action lays in the classification of different risk treatment options. This involves the identification of alternative modes of managing these risks and of integrating

them in a structured set of treatment options. Since identified risks may have varying impact on the organisation, not all risks carry the prospect of loss or damage. Opportunities may also arise from the risk identification process, as types of risk with positive impact or outcomes are identified. So we have to consider Management options for risks expected to have positive outcome, and Management options for risks expected to have negative outcomes.
With the support of the EFR Manager and the Subject Matter expert, the Risk Owner should classify the different risk treatment options.

Development of an action plan
Next, a treatment plan needs to be developed describing how the chosen options will be implemented. The plan should be comprehensive and provide all necessary information about resource requirements, proposed actions, priorities or time plans, roles and responsibilities of partners involved in the action, as well as reporting and monitoring constraints. Besides that, action plans ought to be in line with the values and perceptions of all types of stakeholders (e.g. internal organisational units, outsourcing partner, customers etc.). The better the plans are communicated to the various stakeholders, the easier it will be to obtain the approval of the proposed plans and a commitment to their implementation.

Approval of the action plan
An additional aspect at this point is the approval of the elaborated action plan.
As with all relevant management processes, initial approval is not sufficient to ensure the effective implementation of the process. For this reason the top management of the involved entity should be continuously and properly informed and updated, through comprehensive and regular reporting.

Implementation of the action Plan
The action plan should define how Risk Treatment is to be conducted throughout the organisation. It must be developed in a way that will ensure that Risk Treatment is embedded in all the organisation's important practices and business processes so that it will become relevant, effective and efficient. This means for example that the risk treatment plan should be embedded in the policy development process, in business and strategic planning, and in change management processes.
While implementing the action plan aspects such as the approved activity list, cost indicators and cost reports would also need to be taken into consideration.
Moreover the necessary awareness of the Risk Treatment at the top management levels throughout the implied organisation is mission critical and should receive close attention. Therefore the Risk Owner constantly informs the top management and obtains advice by the Subject Matter Expert.

As a result we could state that a coordinated activity list to implement risk treatment will be generated. Additionally, a project progress report, the implementation of the same, as well as an overview of costs will be the outcome at this point of the EFR Framework.

Identification of Residual Risks
As mentioned before, there is a need to identify any residual risk which might still have to be taking into account at the end of the process. Residual risk is a risk that remains after risk treatment options have been identified and action plans have been implemented. It

also includes all initially unidentified risks as well as all risks previously identified and evaluated but not designated for treatment at that time.
It is important for the organisation's management and all other decision makers to be well informed about the nature and extent of the residual risk. For this purpose, residual risks should always be documented and subjected to regular monitor-and-review procedures.
If the Risk Owner considers a need for further analysis, the evaluated residual risks, should undergo a new *Risk Assessment*, if the evaluated residual risks do not need any further analysis, the next step of the EFR Framework, the *Information Dissemination*, can start.

3.4. Information Management

This part of the EFR Framework deals with the management of information from the collection of relevant information to its dissemination. It includes the *Trend Analysis*, the *Information Collection* and the *Information Dissemination*. The former are ongoing processes which will continuously take place during the performance of the EFR Framework whereas the *Trend Analysis* will be carried out periodically.

3.4.1. Information Collection

The Information Collection is primarily concerned with the identification of information needs to support the EFR Framework, the identification of relevant sources of information to satisfy these needs and the acquisition and review of required information. Expert knowledge is utilized to guide the information acquisition and review activities.
In the following sections a more detailed description of the different activities deployed during the collection of information can be found

At first, the EFR Specialist needs to identify the context of information need which is required to support the EFR Framework. To be able to identify this context he receives information about technologies and validated set of scenarios from the knowledge base and information related to trends. Apart from that, an appointed expert group elaborates an opinion about the context of information need.
Once identified the information need, the Subject Matter Expert obtains input from diverse sources as the World Wide Web, scientific papers, reports, expert opinions, trend reports, etc. The main purpose at this point is to identify and capture sources of information related to the defined context. This list of relevant sources should be incorporated into the knowledgebase from where they can be extracted in order to give a feedback, e.g. when certain scenario has to be formulated.
Besides that, the Subject Matter Expert acquires information about the areas covered by formulated scenarios receiving his input from expert groups or other relevant sources of information.
As a final step the collected information will be reviewed by the Subject Matter Expert and in a further step a report on the effectiveness of information collection method for acquiring relevant and valid information could be developed.

This recurring activity delivers relevant information that will be stored in the knowledge base from where it can be retrieved for example during the *Scenario Building* or the *Risk Assessment*.

3.4.2. Trend Analysis

The result of the Trend Analysis is the creation of current trend reports which serve as a considerable source of information while performing the EFR Framework.
Besides technological and social trends in different areas, trend reports might provide information about upcoming threats, vulnerabilities, threat agents and emerging social and technological values.
At this point of the EFR Framework the trend reports will form part of the Information Collection process. From there they are fed into the *Scenario Building and Analysis* and might as well serve as a source of information for the *Risk Assessment.*

Figure 22: Trend Analysis

The retrieved information is related to trends which we would need to consider. This could be e.g. information concerning emerging and future risks or other relevant fields, or acquired information which includes areas covered by formulated scenarios which had been stored in the knowledge base. Information concerning the development and update of trends should periodically be extracted. The outcome of this activity ought to be used both for scenarios being developed, and for scenarios being stored in the knowledge base.

The work on scenarios might lead to the identification of further emerging threats and vulnerabilities. This information can be retrospectively combined with existing trend reports leading thus to a permanent cycle of updating/expanding the information of the knowledge based management system.

A group of experts is appointed to provide the information related to trends, so that the Subject Matter Expert or the EFR manager can review and analyse these trends in accordance with the support of the Stakeholder Forum and the existing content of the knowledge based management system. The outcome of the expert review of trends will also be passed on to the EFR Manager and it will be stored in the knowledge base for the analysis of upcoming scenarios.

3.4.3. Information Dissemination

For ENISA, output and dissemination are important in order to achieve appropriate Stakeholder involvement. Therefore, after results concerning current and emerging risks

are formulated by ENISA, they should be forwarded to ENISA beneficiaries for their reference as well as for their appropriate action when needed.

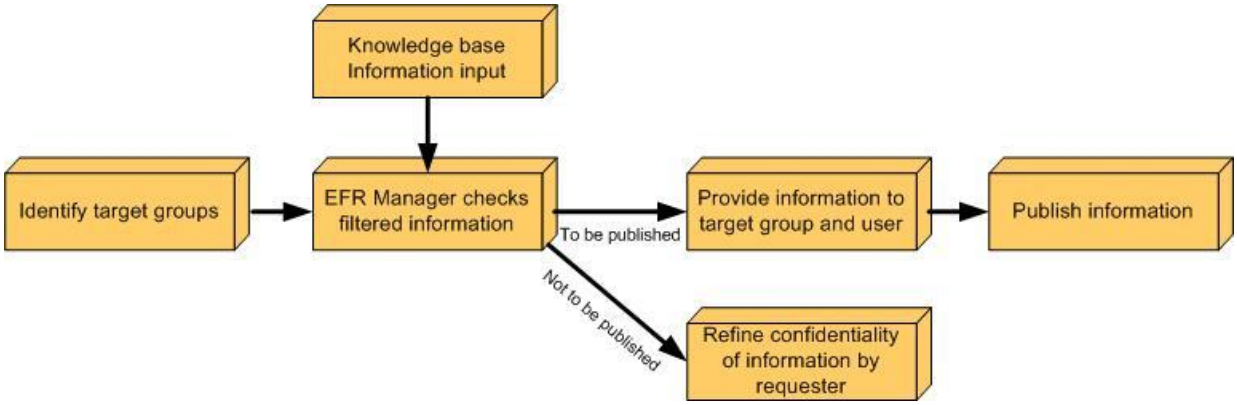

Figure 23: Information Dissemination

The *Information Dissemination* provides the interface between the EFR Knowledgebase developed by ENISA and its target audience. The dissemination starts when new information is inserted. This information is retrieved from the knowledge base and contains the results of the previous Risk Assessment/Risk Treatment activities which were carried out in order to assess possible emerging and future risks within a particular scenario.
The essential idea is to identify the target groups for the information, generate information according to the respective target groups, and provide information to Users based on the relevant access level.
The first task the EFR Manager needs to perform comprises the identification of different target groups that could be interested in receiving information related to the EFR Framework.
Once these target groups have been identified, relevant information is filtered from the Knowledge base and checked by the EFR Manager.
At this point the EFR Manager needs to decide whether the information can be made public or not. Supposing that the information can be made public and there are no requirements in terms of confidentiality established in the request, the filtered of information could be provided to the identified target group. Please note that classified information will only be retrievable from the knowledge base according to the access level granted to the User.
The results of the *Risk Assessment* activity elaborated for particular requests can be published using diverse dissemination mechanisms which could be applied to different time lines:

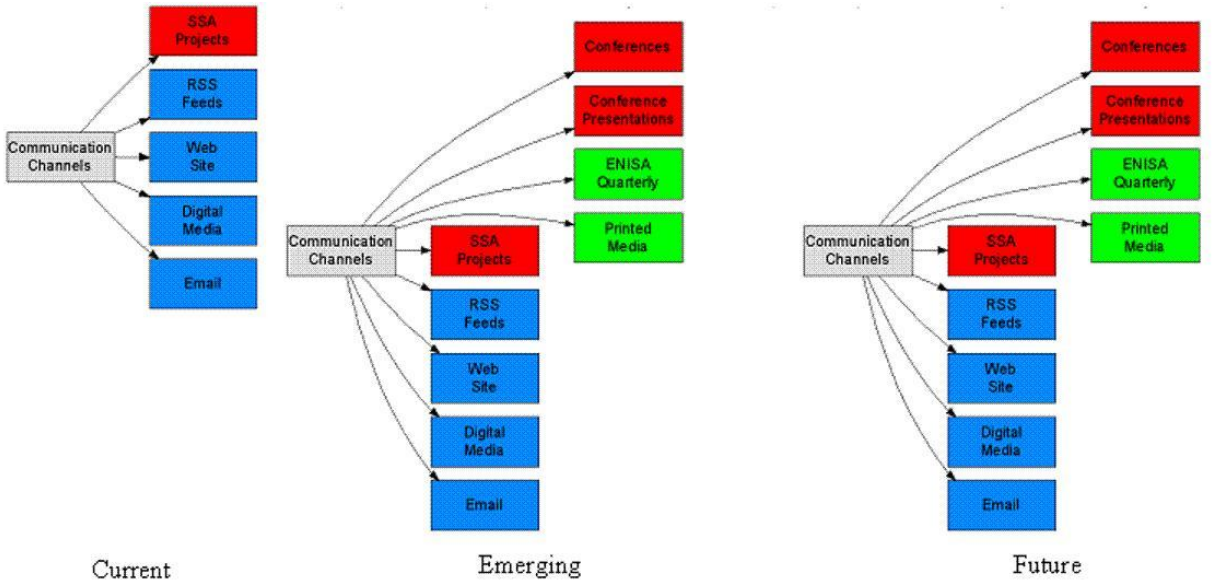

Figure 24: Dissemination mechanisms

The stated list below includes available communication mechanisms and channels through which the results of the ''Risk Assessment'' can be disseminated:

- **Email lists** where relevant information will be sent periodically. We envision needing the following lists for the dissemination:
  - A list of contacts for Member States
  - A list of contacts for the EU institutions
  - A list of contacts for members of the industry
  - A list of contacts for the academic research institutions
  - A list of contacts for any other ENISA beneficiaries?
  - A list of contacts for the media and the press?
- A **Website** where the RA reports will be posted
- **ENISA Quarterly** or **ENISA Newsletter** could also be used to disseminate summary versions of the RA reports.
- ENISA may also create **focused leaflets** and similar advertising material
- **High-profile digital media** for publishing summaries of the RA reports, including well known radio and TV stations in European countries. It is advisable to consider channels which are broadcast in more than one country, or even better, channels that have a clear European dimension, such as Euro news, etc.
- **High-profile printed media** for publishing summaries of the RA reports. Again, it is advisable to consider widely published technical/professional publications, which are published in more than one country, and/or which have a clear European dimension.
- Presentations of the RA results in relevant **conferences**, or even co-organise such events.
- Close **cooperation with other projects** focusing similar subject matter

Depending on the urgency of information to be delivered, different channels are appropriate. Indeed, if the information is urgent we need to send it using fast and immediate communication channels, such as email, Web Sites, Digital Media, etc.

In case that the requestor demands confidentiality, the request needs to be returned to him inquiring to define precisely which information can be published and which not.
More information can be found in Annex I - Information dissemination for private information.

Output of this activity:

- Target group for information
- Filtered information
- Information to user

4. Maintenance of the EFR Framework

4.1. Introduction

Projects are, by definition, limited in time Projects create business outcomes that need regular, ongoing attention in order to operate efficiently and effectively over the long term. In many cases, the project team does not retain responsibility for the product after delivery. The type, and often the pace, of work associated with maintenance are different than during development and implementation. The need to manage change continues but may continue in a different form. Governance structures are different once the project ends.

Without advance agreement on how the product will be maintained, who will have responsibility for maintenance, how maintenance priorities will be set and maintenance activities governed, the project could successfully implement something that quickly becomes obsolete or unused.

4.2. EFR Framework Maintenance Plan

Keeping the EFR Framework current and of high quality is a key factor in order to maintain its relevance and usefulness. Therefore the establishment of a maintenance plan as a useful tool to support ENISA scheduling the important tasks of keeping the EFR Framework updated in the future. Thus, after the EFR Framework has been set up, the following activities form part of the maintenance plan:

4.2.1. Management of groups

Physical and virtual teams will participate in the EFR Framework. The EFR Framework should ensure that the geographically dispersed teams work together as a single team. To this end, the definition of a responsible for the group management is very important. The EFR Manager will take this role, managing the membership, their tasks and what resources they can access. His/her main tasks would be:

- Establish the different groups that will participate in the EFR Framework
- Add, delete and modify people of the different groups
- Assign names to roles based on the people's availability as well as on the expertise and knowledge
- Update the assignment of tasks (i.e. if a member left the EFR Framework, the EFR Manager would assign the tasks to another person)
- Provide people with access to the different resources according to their privileges

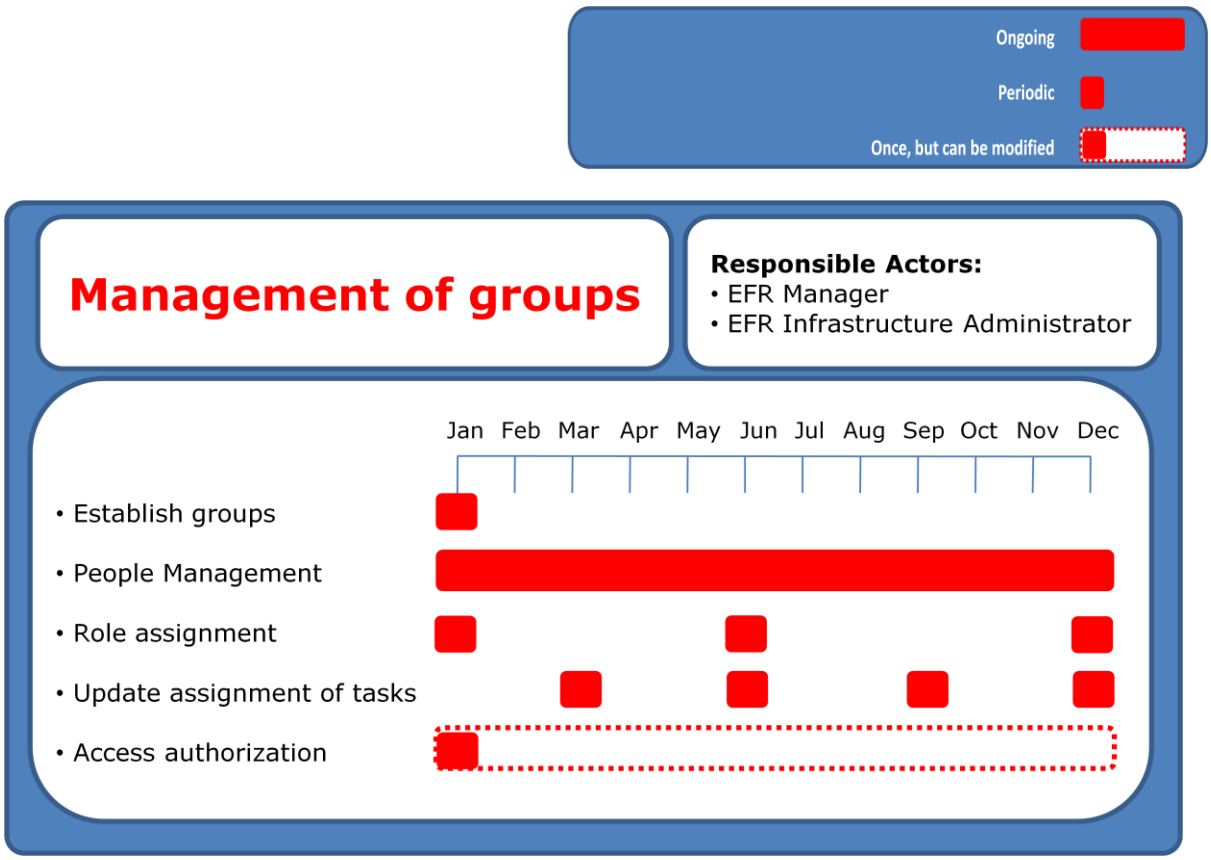

Figure 25: Maintenance – Management of groups

The EFR Infrastructure Administrator will implement the day to day group changes requested by the EFR Manager in the platform, increasing the overall integrity of the policy.
On the other hand, effective interpersonal communication among members of the same group and successful communication with managers are critical components of team functioning. Thus, the EFR Manager will be responsible for the organisation of frequent meetings between the members of the different groups. Goals, objectives and minutes of the meetings should be also delivered by the EFR Manager. Further information about the meetings may be found in the "EFR Organisation and Implementation" chapter.

4.2.2. Document Management

The document management in the EFR Framework should provide storage, versioning, metadata, and security as well as collaboration capabilities:

- *Storage* of the documents that includes where they are stored, for how long, migration of the documents and eventual document destruction.
- Managing the content of the knowledge base. This includes the maintenance of documents generated during the scenario processing as well as those deriving from

the outside (e.g. trend reports). The stored information in the knowledge might be subject to changes and requires adequate updating.

- *Metadata* that includes for example the date the document was stored and the identity of the user storing it.
- *Security* is important in the EFR Framework. The EFR Infrastructure Administrator will give access to documents, depending on the type, to only certain people, roles or groups of people following the instructions of the EFR Manager.
- *Version control* allowing users to retrieve previous versions and to continue work from a selected point. Versioning is very useful for scenario building since the scenario documents will change over the time and require updating. Moreover, it will be very useful once a necessity might arise to go back to a previous copy.
- *Collaboration*: Documents should be capable of being retrieved by an authorized person and worked on. Access should be blocked to other users while work is being performed on the document. For instance, a scenario document should be blocked to other experts while an expert is working on it.

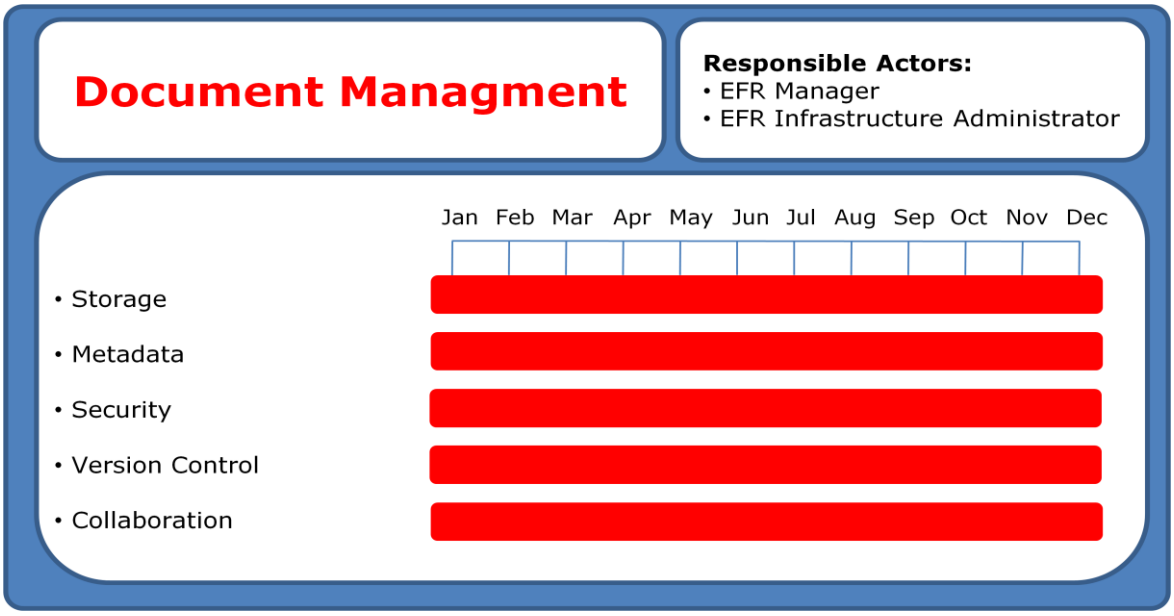

Figure 26: Maintenance – Document Management

4.2.3. Monitoring

Monitoring encompasses the tracking of individual processes so that information on their state can be easily seen and statistics on the performance of one or more processes provided. An example of the tracking could be the status of a user request (i.e, request validated, scenario of the request created, risk report on the request created, etc.) so that problems in its operation can be identified and corrected.

In addition, this information can be used by the requestors and experts to improve their connected processes. Examples of statistics are the generation of measures on how

quickly a user request is processed or how many requests are processed in the last month. These measures tend to fit into three categories: cycle time, defect rate and productivity.

The degree of monitoring depends on what information the EFR Framework wants to evaluate and analyse and how the EFR Framework wants it to be monitored, in real-time or ad-hoc.

The event logs extracted through process monitoring may be analysed and they can be compared with an 'a priori' process model. In this way, the EFR Manager may detect discrepancies between the actual EFR Framework execution and the a priori workflow as well as to analyse bottlenecks.

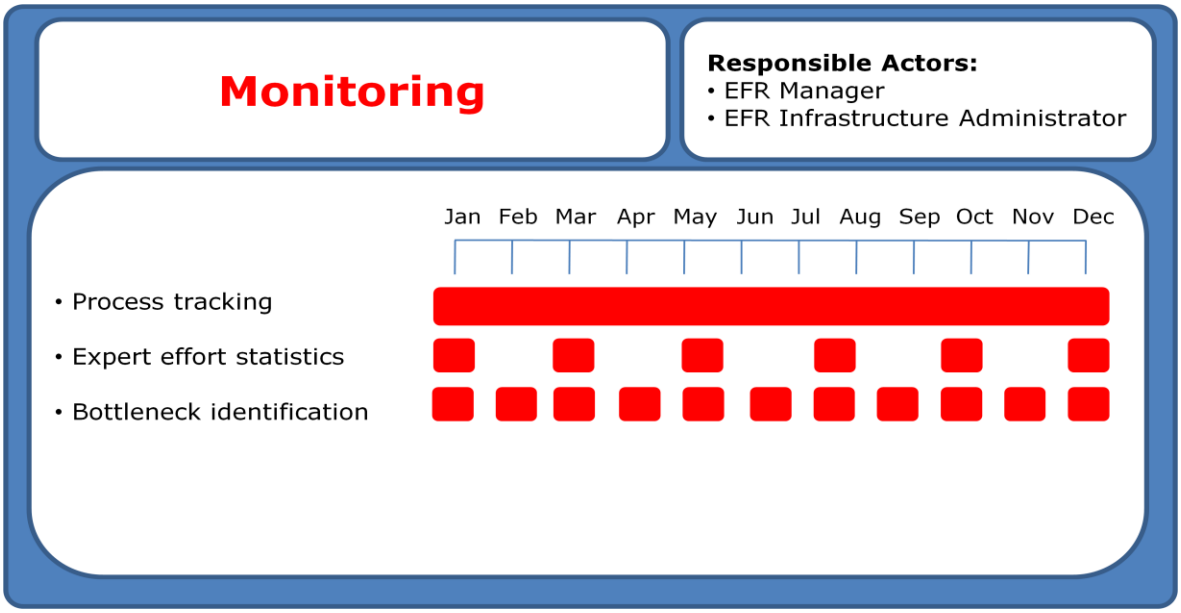

Figure 27: Maintenance – Monitoring

It could be suggested that the EFR Manager performs different types of monitoring at least once every two weeks in order to reduce bottlenecks and keep the EFR Framework running smoothly. Examples of tests would be:

- How quickly a request is processed
- How many requests are processed in a month?
- How many weeks are necessary to build a scenario?
- How many experts take part in the scenario building?
- How much time is needed for the analysis of a scenario?
- Productivity of the different people involved in the EFR Framework.

The main benefits of these reports on process statistics are:

- Identifying and eliminating bottlenecks within the EFR Framework organisation
- Building, refining and streamlining mission critical parts of the EFR process
- Improving how key information is routed within the EFR Framework

- Removing frustrating bottlenecks and improving EFR processes that directly impact ENISA bottom line.

4.2.4. Optimisation

The EFR Framework optimisation includes retrieving the framework performance information from the monitoring phase and identifying the potential or actual bottlenecks as well as potential rooms for cost savings or other improvements. Then, those enhancements should be applied to the design of the workflow process or to the tasks people are assigned to.

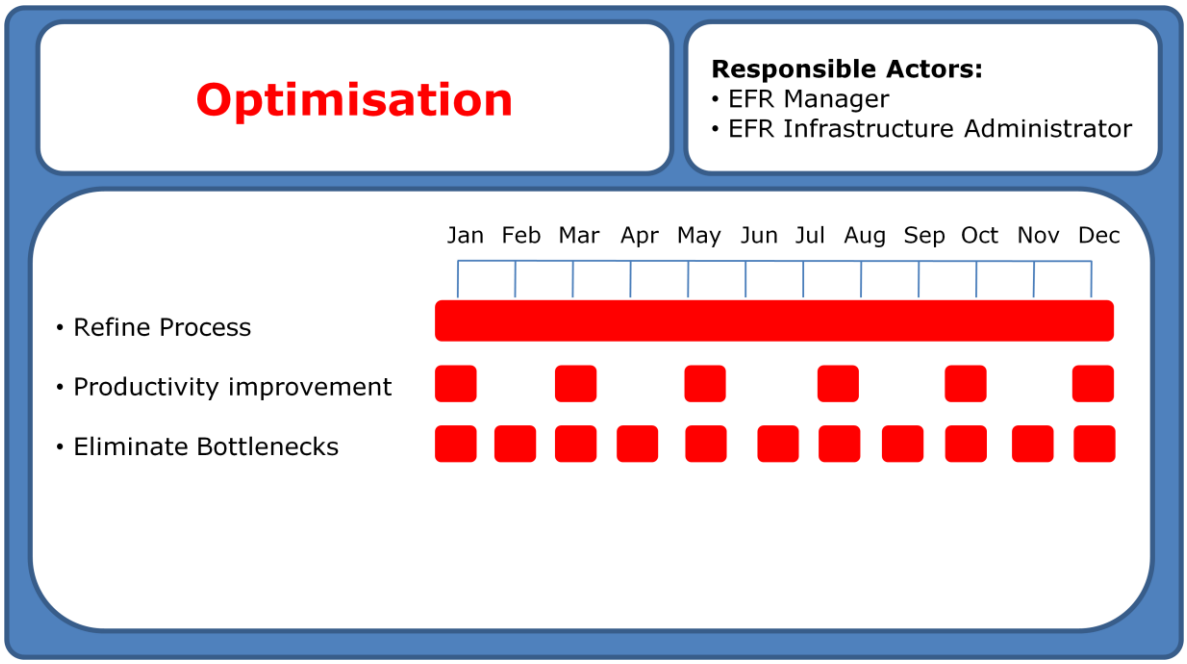

Figure 28: Maintenance – Optimisation

4.2.5. Technical Maintenance of required IT Components

Technical maintenance is a large component of the overall maintenance of the EFR Framework. The EFR Infrastructure Administrator will help ENISA prevent problems with the platform on which the EFR Framework is going to be implemented.
Based on categories, there are different types of IT maintenance the administrator should plan:

- *Hardware maintenance*: Testing and cleaning of the hardware
- *Software maintenance*: Updating of the chosen platform in order to meet changing information requirements, such as adding new functions. It also includes fixing bugs and adapting the software to new hardware devices.

- *Network maintenance*: Taking care of the overall health of the network (anticipating, preventing and solving the problems, troubleshooting, cable testing)
- *Security maintenance*: Ensuring that the systems remain secure all the time. Security maintenance service may include backups, checking permissions and ownerships in critical files and directories, checking the assignment of rights, monitoring system logs etc.

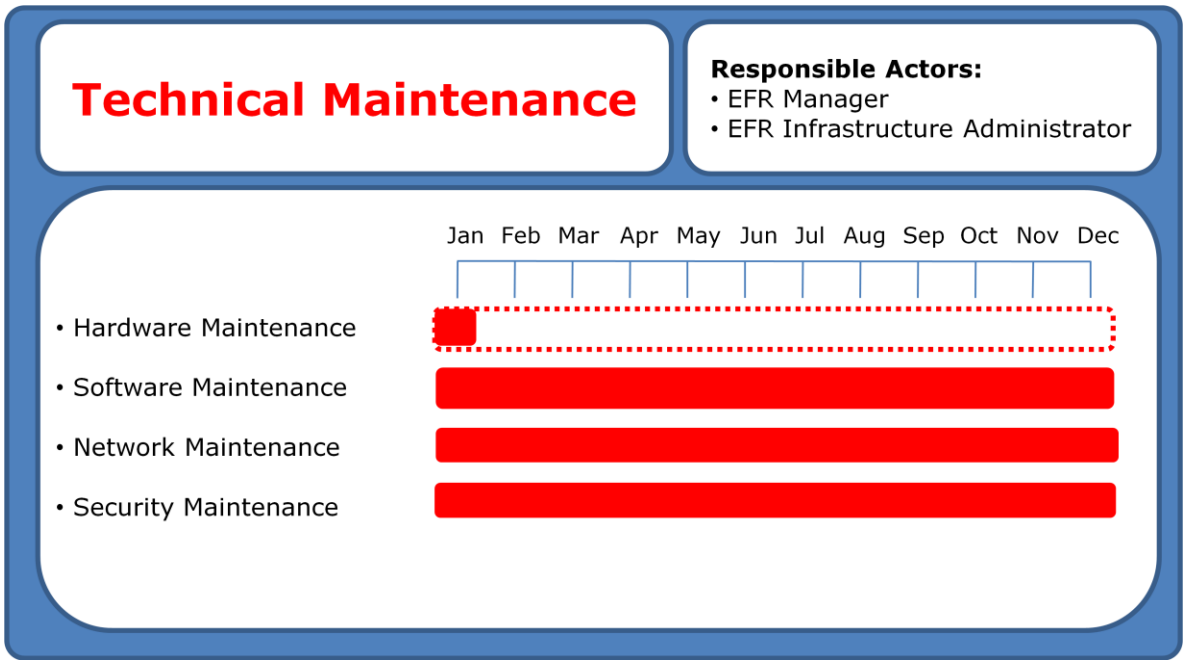

Figure 29: Maintenance – Technical Maintenance

Glossary

Ref.	Term	Description
1	**Acceptable Risk**	The level of residual risk that has been determined to be a reasonable level of potential loss/disruption for a specific system. (CIAO – Critical Infrastructure Assurance Office - U.S.A)
2	**Accountability**	The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO/IEC PDTR 13335-1) This may cover non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (ENISA)
3	**Asset**	Anything that has value to the organisation, its business operations and their continuity, including Information resources that support the organisation's mission. (ISO/IEC PDTR 13335-1)
4	**Consequence**	Outcome of an event There can be more than one consequence from one event. Consequences can range from positive to negative. Consequences can be expressed qualitatively or quantitatively (ISO/IEC Guide 73)
5	**Contingency Plan**	A plan for emergency response, backup operations, and post-disaster recovery in a system, as part of a security program, to ensure availability of critical system resources and facilitate continuity of operations in a crisis. (ENISA)
6	**Current risk**	Risks that from a risk management point of view are relevant within the timeframe of present time up to one year. ENISA
7	**Data Availability**	The fact that data is accessible and services are operational. (ENISA)
8	**Data Confidentiality**	The protection of communications or stored data against interception and reading by unauthorized persons. (ENISA) The property that information is not made available or

Ref.	Term	Description
		disclosed to unauthorized individuals, entities, or processes. (ISO/IEC PDTR 13335-1)
9	**Data Integrity**	The confirmation that data which has been sent, received, or stored are complete and unchanged. (ENISA) The property that data has not been altered or destroyed in an unauthorized manner. (ISO/IEC PDTR 13335-1)
10	**Definition of Scope**	Process for the establishment of global parameters for the performance of Risk Management within an organisation. Within the definition of scope for Risk Management internal and external factors have to be taken into account. (ENISA)
11	**Disaster Recovery**	The process of restoring a system to full operation after an interruption in service, including equipment repair / replacement, file recovery / restoration. (ENISA)
12	**EFR Framework**	A scenario-based process model developed in order to assess and manage Emerging and Future Risks.
13	**Emerging Risk**	Risks that from a risk management point of view are relevant from one year to five years out. ENISA
14	**Event**	Occurrence of a particular set of circumstances The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences. (ISO/IEC Guide 73)
15	**Evidence**	Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Evidence does not necessarily prove truth or existence of something but contributes to establish proof. (ENISA)
16	**Exposure**	The potential loss to an area due to the occurrence of an adverse event. (ISACA) Generally, in the Risk Management process a risk does

Ref.	Term	Description
		not always represent a loss or a negative consequence but can also be an opportunity or a result of a positive event. (ENISA)
17	**Future Risk**	Risks that from a risk management point of view are relevant beyond five years out. ENISA
18	**Gap Analysis**	A comparison that identifies the difference between the actual and the expected / specified system status. (ENISA)
19	**Impact**	The result of an unwanted incident. (ISO/IEC PDTR 13335-1)
20	**Impact Analysis**	The identification of critical business processes, and the potential damage or loss that may be caused to the organisation resulting from a disruption to those processes. Business impact analysis identifies: - the form the loss or damage will take - how that degree of damage or loss is likely to escalate with time following an incident - the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level - the time for full recovery of the business processes (ENISA)
21	**Incident**	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system. (ENISA)
22	**Interested Party**	Person or group having an interest in the performance or success of an organisation's mission or objectives. (ISO/IEC Guide 73)
23	**Mitigation**	Limitation of any negative consequence of a particular event. (ISO/IEC Guide 73)
24	**Monitor and Review**	A process for measuring the efficiency and effectiveness of the organisation's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with

Ref.	Term	Description
		decisions.(ENISA)
25	**Priority**	Sequence in which an incident or problem needs to be resolved, based on impact and urgency. (ENISA)
26	**Probability**	Extent to which an event is likely to occur. (ENISA)
27	**Procedure**	A written description of a course of action to be taken to perform a given task.(ENISA)
28	**Process**	An organized set of activities which uses resources to transform inputs to outputs.(ENISA)
29	**Process Owner**	An individual held accountable and responsible for the workings and improvement of one of the organisation's defined processes and its related sub-processes. (ENISA)
30	**Residual Risk**	Risk remaining after risk treatment. (ISO/IEC Guide 73)
31	**Risk**	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. (ISO/IEC PDTR 13335-1)
32	**Risk Acceptance**	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. (ISO/IEC PDTR 13335-1) -Risk acceptance depends on risk criteria defined within the process Definition of Scope. (Definition adopted from ISO/IEC Guide 73 with some modification by ENISA)
33	**Risk Analysis**	Systematic use of information to identify sources and to estimate the risk. - Risk analysis provides a basis for risk evaluation, risk treatment and risk acceptance. (ISO/IEC Guide 73)
34	**Risk Assessment**	A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation. (ENISA)
35	**Risk Avoidance**	Decision not to become involved in, or action to withdraw from, a risk situation. (ISO/IEC Guide 73)

Ref.	Term	Description
36	**Risk Communication**	A process to exchange or share information about risk between the decision-maker and other stakeholders. - The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk. (ISO/IEC Guide 73)
37	**Risk Control**	Actions implementing risk management decisions. - Risk control may involve monitoring, re-evaluation, and compliance with decisions. (ISO/IEC Guide 73)
38	**Risk Criteria**	Terms of reference by which the significance or risk is assessed. - Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic aspects, the concerns of stakeholders, priorities and other inputs to the assessment. (ISO/IEC Guide 73)
39	**Risk Estimation**	Process used to assign values to the probability and consequences of a risk. - It can consider cost, benefits, the concerns of stakeholders and other variables, as appropriate for risk evaluation. (ISO/IEC Guide 73)
40	**Risk Evaluation**	Process of comparing the estimated risk against given risk criteria to determine the significance of risk. (ISO/IEC Guide 73)
41	**Risk Financing**	Provision of funds to meet the cost of implementing risk treatment and related costs. (ISO/IEC Guide 73)
42	**Risk Identification**	Process to find, list and characterize elements of risk. (ISO/IEC Guide 73)
43	**Risk Management**	The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention

Ref.	Term	Description
		and control options. (ENISA)
44	**Risk Optimisation**	Process, related to a risk to minimize the negative and to maximize the positive consequences and their respective probabilities. - Risk optimization depends upon risk criteria, including costs and legal requirements. (ISO/IEC Guide 73)
45	**Risk Perception**	Way in which a stakeholder views a risk, based on a set of values or concerns. - Risk perception depends on the stakeholder's needs, issues and knowledge. - Risk perception can differ from objective data. (ISO/IEC Guide 73)
46	**Risk Reduction**	Actions taken to lessen the probability, negative consequences or both, associated with a risk. (ISO/IEC Guide 73)
47	**Risk Retention**	Acceptance of the burden of loss, or benefit of gain, from a particular risk. - Risk retention includes the acceptance of risks that have not been identified. - Risk retention does not include treatments involving insurance, or transfer by other means. (ISO/IEC Guide 73)
48	**Risk Transfer**	Sharing with another party the burden of loss or benefit of gain, for a risk. - Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk. - Risk transfer can be carried out through insurance or other agreements. - Risk transfer can create new risks or modify existing risk.

Ref.	Term	Description
		(ISO/IEC Guide 73)
49	**Risk Treatment**	Process of selection and implementation of measures to modify risk. - Risk treatment measures can include avoiding, optimizing, transferring or retaining risk (ISO/IEC Guide 73)
50	**Safeguards**	Practices, procedures or mechanisms that reduce risk. - The term 'safeguard' is normally considered to be synonymous with the term 'control'. (ISO/IEC PDTR 13335-1)
51	**Security**	All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. - A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. (ISO/IEC WD 15443-1)
52	**Source**	Item or activity having a potential for a consequence. (ISO/IEC Guide 73)
53	**Source Identification**	Process to find, list and characterize sources. (ISO/IEC Guide 73)
54	**Stakeholder**	Any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by, a risk. (ISO/IEC Guide 73)
55	**Threat**	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (ENISA)
56	**Vulnerability**	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved. (ITSEC)

Annex I - Complementary information on the EFR Framework

CAPTURE USER REQUEST

After having granted the level of access to the user, the EFR Manager will obtain the most appropriate template from the knowledge based management system in order to proceed with the request. The template is forwarded to the Requestor who will fill it out with his/her requirements. Afterwards the EFR Manager validates and formats the requests accordingly. This includes that he would need to verify if the needed documentation is completely presented.

By means of this template client-specific requirements are properly formatted and presented in a structured way. Finally, the Requestor will be informed that his request has been accepted.

Output of this activity:

Validated and properly formatted requests

(More information on the input and output of these activities can be found in Annex II - Related input and output of activities)

VALIDATION OF SCENARIO DESCRIPTION

The purpose of this action is to ensure that the generated scenarios are valid and useful for the risk assessment exercise. Experts will review these scenarios and make appropriate decisions on their validity.

If valid, the generated scenarios are then approved by the EFR Stakeholder Forum. Otherwise, the scenarios may need to be reworked again. The following steps will lead to the validation of scenarios:

1. Expert review of scenarios:

First, the EFR Expert groups need to review the scenario and provide feedback. Likewise the Subject Matter Expert should receive feedback from the Requestor concerning the elaborated scenario descriptions, by this means it ought to be ascertained that the scenario description is in line with the expectations of the User.

Assuming the scenarios might not be valid, the settings of the scenarios would need to be reworked again. Therefore, they would need to pass once more through the Scenario Building and

Input of this activity:

- Description of a set of scenarios

Output of this activity:

- Feedback and consultation
- Feedback and decision on whether the scenarios are valid or not

Analysis before re-entering the review stage.

2. Confirming the validity of scenario description:

Once the review and consulting of the scenario is completed, the responsible experts decide whether the prescribed scenarios are valid or not.
In order to make a decision on the validity of a scenario, the EFR Specialist has to identify the skills required of experts that will undertake these tasks. With this list of skills the HR Staff can select and appoint experts (Subject Matter Experts) capable of undertaking the required tasks such as generating and validating scenarios.

Supposing that the approval of the scenarios is assured, the scenarios would be validated by the EFR Stakeholder Forum and developed along with Subject Matter Experts. Their validity ensures that these scenarios are relevant and useful. Accordingly the User will be informed that his request has been accepted.

Should the validation of the scenarios not be conceded, the EFR Specialist would receive appropriate feedback in order to refine the scenario description.

(More information on the input and output of these activities can be found in Annex II - Related input and output of activities)

INFORMATION DISSEMINATION FOR PRIVATE INFORMATION

In the case that the information cannot be made public, the EFR Manager supported by the authentication system ought to verify the user's identity information and establish the level of access to classified information which has been granted to the User. Please note that at this point the term User does not refer necessarily to User in the sense of Requestor, which means that User here implies the entity or person who will actually use the information.

Assuming that access to classified information is permitted, the User can acquire information from the knowledge based management system regarding his specific requirements and granted access level. This process is supervised by the EFR Manager and includes that the information would need to be filtered according to the user's requirements and his access control rules. Subsequently the so acquired information and the access rights of the Users will be compared, before presenting the information to the User via a public area or email notification.
As an outcome, the information can be disseminated to the public via different channels described in the chapter of ''Information Dissemination''.

Input of this activity:
- Filtered requested data
- Information request form
- User identity data
- User's information requirements

Output of this activity:
- Requested data
- Information to user

Should the access of the User to classified information be denied, the EFR Manager redirects the User to the Terms and Conditions and the public Website.
In the following, the EFR Manager acquires unclassified information from the Knowledgebase management system taking into account the user-specific requirements and his granted access level.
The so achieved unclassified information will as well be presented to the User and published as indicated in the ''Information Dissemination''.

(More information on the input and output of these activities can be found in Annex II - Related input and output of activities)

Annex II – Related input and output of activities

Description of a set of scenarios
Text based scenario description, i.e. this description does not contain a scenario in the structured format, it describes for example, actors, timeframe, technologies / applications, context, used information, etc. in prose form. This description can come from the requestor or alternatively the EFR Specialist and the requestor construct it cooperatively. (E.g. Word or PDF document)

Description of a set of scenarios with the appropriate RM results
This data object is a result of the Refine scenario descriptions based on RM results activity. Thus, this data is produced when the feedback loop from the risk management phase is utilized. Data object contains appropriate results from the RA and RT phases, and thus its access rights can differ from the initial scenario description (Description of a set of scenarios)

Filled scenario template
The scenario is described in a template form. EFR Specialist and Subject Matter Expert identify items from Description of a set of scenarios and fill them to the Scenario template. Probably, all fields are not filled in (depends on scenario description).

Feedback
Feedback data that is collected from the Requestor in the Validation of the scenario description phase. Free formatted text that contains comments and refinement suggestions related to description of a set of scenarios. Contains at least:

- Requestor's identification information
- Data and time
- Name of the reviewed document
- Feedback

Feedback and decision on whether the scenarios are valid or not
This data goes back to the Scenario building from Validation of scenario description. Free formatted text that contains comments and refinement suggestions related to Description of a set of scenarios. The Subject Matter Expert produces this data based on Feedback and Feedback and consultation data. Contains at least:
Identification information of the feedback giver

- Data and time
- Name of the reviewed document
- Feedback

Feedback and consultation
Feedback and consultation from the EFR expert group in the Validation of the scenario description phase. Free formatted text that contains comments and refinement suggestions related to description of a set of scenarios. It contains at least:

- Expert group's identification information
- Data and time
- Name of the reviewed document
- Feedback

Filtered information
This is information that can be made available to the target group. This means that information is arranged based on access rights {public, internal, confidential}.
N.B. all information from the knowledge based management system can be disseminated if the User has sufficient rights.

Filtered requested data
This is the data object that is got when the Requested data object is filtered according to access rights. Thus, from this data the Information management system produces Information to user data element, i.e. data presented for User

Information request form
Query input relevant to the form (for example there can be drop-down menu for technologies in the form)

- Technology
- Application
- Key words

Information to user
Output from the Information dissemination, i.e. the information set that is delivered to the user. This data varies relating to user's access rights and User's information requirements.

Request acceptance info
A reply message is send to the requestor that her/his request is accepted, a related description of a set of scenarios is ready for analysis. EFR Manager sends this in Formulate scenarios or Use given scenario phase.

- Request's name
- Acceptance date

Request template
Is an empty template for capturing user's scenario request in a structured format. The template has to contain at least:

- User identity data
- Technology
- Application
- Description of the technology and the application
- Justification / reason why it is important to consider the specific technologies / application
- What kind of RT is wanted
- Access rights for the information related to this request

The following information is not mandatory, but helps the RM phase if available.

- Impact statement, i.e. the importance for assets
- Asset classification scheme
- Suggestion for the used Risk id methodology
- Existing controls

Request in template
A request template filled by the Requestor

Requested data
This data is queried from the knowledge based management system based on the User's information requirements data object. Therefore, this information can contain any available information from the knowledge base (NB: access rights are checked later on)

RM results
The results of the Risk Assessment and Treatment phases. This data object can be disseminated if the requestor has given permission. In addition, this data object is used to refine scenario descriptions when the feedback loop from the RM phase to the Scenario building is exploited.

Scenario template
Please find example in Annex III. The purpose is that all necessary information from the validated description of a set of scenarios data object can be presented in this template form. Contains at least:

- Asset
- Context
- Technology / application
- Timeframe
- Data
- Used Subject Matter Expert

Selection
The selected Subject Matter Experts. List of expert names and their organisations.

Target group for information
A list of user names, organisations etc. Also access rights (public, internal, confidential) are taken into account in this data element.

Trend reports
E.g. Word / PDF documents or web sites

User identity data

- User name
- Organisation
- Sector
- Role in the organisation
- Role in the workflow
- Access rights

User's information requirements
In the Information dissemination for private information the User defines his/her information needs and this data element contains these needs. Based on this data element search for the knowledge base is executed.

Validated and properly formatted request
Validated and accepted user request in a request template. Output from the Capture user request.

Validated description of a set of scenarios
Description of a set of scenarios data object that the expert group is reviewed and accepted. Output of the Formulate Scenarios or Use Given scenario. Thus, contains the same information as the description of a set of scenarios and in addition the acceptance date.

Annex III –Template

Structure of the template

The template is structured as follows:

- Introductory part, where a general overview and the background of the scenario idea is provided
- The Scenario description, including the following information:
  - *Scenario type*: explorative or predictive [in our case is predictive]
  - *Scenario raw description*: this is where we the scenario is described in free text.
  - *Assumptions*: Any assumptions made while formulating the scenario.
- "Framing the scenario" section contains a number of fields, with information we would like to know. Since as you will see most of this information required may be already included in the raw description, this section is actually offered as an alternative, in case experts instead of providing a free text, rather prefer to introduce their input directly to a more structured template. This would also provide us with specific information we need for the Analysis phase.
- "Analysing the scenario" section: it is where the Scenario Analysis takes place. This is actually a borderline between the actual scenario analysis and risk assessment of the specific technology / applications we have chosen. We have included methodological items we would need to consider in order to perform the assessment (such as assets, threats, vulnerabilities, impact etc).
- A Glossary / Aid, where important terms like "threats", "vulnerabilities" etc are defined and more information is provided so that you are able to fill it in.
- Other information, where more information not specified in the table above could be specified, or figures and picture added etc.
- References, where all references used for the completion of the tables should be listed.

EFR Application Scenario – [Title]

[Introductory text]

[Title]

Type of scenario flow *["predictive" or "explorative" to indicate the nature of the scenario]*	*Predictive*: what will happen
Raw description of scenario [*who does what* or *what happens*]	
Assumptions *[any assumptions made while writing the scenario flow. Assumptions is a place holder for information that may concern generic information about relevant legislation, devices, applications, participants, etc.]*	
1. 2. 3. 4.	

Framing the scenario	
Timeframe [*when the scenario takes place]*	
Location [*where: Home / work / public space...*]	

Actors [*who: entities relevant to the scenario and describe their roles and goals. These most probably include humans and organizations and NOT IT systems.]*	• •
Technologies / devices [*technologies / devices used in the scenario*]	• •
Applications [*applications used in the scenario*]	•
Data *[information that is collected, or flows through the network, or is being stored and further processed]*	•
Drivers *[key drivers behind the scenario: socio-economic, political, environmental or personal motivation...]*	•

Analysing the scenario

A. Assets
[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
Intangible				
A1.				
A2.				
A3.				
A4.				
A5.				
Tangible				
A6.				
A7.				
A8.				

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
V1.			
V2.			
V3.			
V4.			
V5.			
V6.			

Analysing the scenario			
C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*			
	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
C1.			
C2.			
C3.			

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
T1.					
T2.					
	[1] Note that the same threat may exploit more than one vulnerability of the same or different assets. ***[2] In case the threat is of human origin; if it is an environmental threat (like earthquake, fire etc.), you do not need to fill this in.***				

Analysing the scenario

E. Impact *[estimation of impact of the identified threats; it is closely related to the asset value, so you need to consider that]*

No.	Impact	Description
Legal and Ethical		
I01		
I02		
I03		
Social and Political		
I04		
I05		
I06		
I07		
Health		
I08	Loss of Life	
I09	Health Deterioration	
Financial / Economical		
I10		
I11		
Organisational / Technological		
I12		
I13		

Analysing the scenario

F. Acceptable risk level *[estimation of levels of risk that are derived from the subject matter area and concern above assets, vulnerabilities and impacts. The risk level are classified via a scale from 1-10]*

Acceptable risk level *[Scale 1-10]*	**Asset (s) considered** [*same as in assets above*]	**Value of the considered asset** *[same as in asset field above]*	**References** *[reference to existing practices, regulation, subject matter]*

Analysing the scenario
G. Assumptions *[any assumptions made during the analysis, i.e. identification of vulnerabilities, threats, impact etc.]*

Glossary / Aid

Here are some definitions of the terms / concepts according to ISO/IEC 13335-1 (2004)[1] and the Glossary in ENISA Web-site[2] that you see are required to be filled in the table above and which will help you fill in the table.

Asset – Anything that has a value to the organisation (note: in our case not only the organisation...). These assets have value to the organization, which is normally expressed in terms of the impact on business operations from unauthorized disclosure, modification or repudiation of information, or unavailability or destruction of information or service.

Vulnerability - A weakness of an asset or group of assets that can be exploited by one or more threats. Refers to an aspect of a system that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance or attack. A vulnerability can exist in the absence of corresponding threats and in itself it does not cause harm; a vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Vulnerabilities arising from different sources need to be considered, for example, those intrinsic or extrinsic to the asset.

Threat – An activity or event the occurrence of which could have an undesirable impact; the circumstance or event has the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats may be of environmental or human origin and, in the latter case, may be either accidental or deliberate. Statistical data are available concerning many types of environmental threats. Such data may be obtained and used by an organization while assessing threats. Threats have characteristics that define their relationships with other security elements. These characteristics may include the following:

- motivation, e.g. financial gain, competitive advantage,
- frequency of occurrence,
- likelihood, and
- impact

Impact - The loss or degradation of a business value (money, reputation, trust etc.) or any other loss that could have been the consequence of a particular violation. Impact is the result of an information security incident, caused by a threat, which affects assets. The impact could be the destruction of certain assets, damage to the ICT system, and compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Possible indirect impact includes financial losses, and the loss of market share or company image.

---

[1] *ISO / IEC 13335-1 (2004) "Information technology - Security techniques - Management of information and communications technology security — Part 1:Concepts and models for information and communications technology security management"*

[2] *http://www.enisa.europa.eu/rmra/glossary.html*

Other information

[You may provide here other information you consider relevant and cannot be covered in the fields above, e.g. images etc.]

References

Annex IV - Input/output RA/RT

	Input Data	Output Data
Activity	**Risk Assessment**	
Identification of risks	Impact statement Historical information Risk ID methodology Assessment tools	Disregarded threats just. Likelihood data Identification method doc values Relevant vulnerabilities Relevant impacts Relevant threats
Analysis of relevant risks	Relevant vulnerabilities Risk limits Asset class. Scheme Disregarded threats just. Identification method doc. Relevant threats Likelihood data Existing controls Relevant impacts Relevant detailed assets Values	Impacts relative to assets Threats relative to assets Classified assets Controls relative to assets Risk relative to assets Risk relative to asset groups
Evaluation of risks	Controls relative to assets Impacts relative to assets Assessment activities criteria Threats relative to assets Risks relative to asset groups Classified assets Assets class. Scheme Risks relative to assets	Risk treatment decision
Activity	**Risk Treatment**	
Identification of options	Assessment activities criteria Risk treatment decision Risk limits for criteria Risk treatment options	Class. Risk treatment options
Development of action	Priority scheme	Responsibility assignment

plan	Add org. roles Planning methodology Class. Risk treatment options	Resource assignment Action plan
Approval of action plan	Presentation techniques Action plan	Approved Activity Lists
Identification of residual risks	Internal stakeholder events	Evaluated residual risks