

Emerging and Future Risks Workflow



and

**Jeremy Hilton,
Pete Burnap and Anas Tawileh
Cardiff University**

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

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

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

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© European Network and information Security Agency (ENISA), 2007

Contents

1	Introduction	1
1.1	Background	1
1.2	EFR Process	1
1.3	Structure of this document	1
2	Development Approach	2
2.1	Phase 1	2
2.2	Phase 2	3
2.3	Phase 3	4
3	Process Model	5
3.1	The EFR Lifecycle	5
3.2	The EFR process model	6
3.2.1	Submission of Requests	7
3.2.2	Scenario Building	8
3.2.3	Validation of Results	9
3.2.4	Trend Analysis	10
3.2.5	Information Collection	11
3.2.6	Information Dissemination	12
3.2.7	Validation of Methods	13
3.2.8	Risk Assessment	14
3.2.9	Risk Treatment	15
3.3	Organisational Roles	16
	Annex A Activity Analysis	A-1
	Annex B Role Analysis	B-1
	Annex C Icons used within Processes	C-1

Emerging and Future Risk Process

1 Introduction

1.1 Background

ENISA requires support in continuing and expanding its work on the field of assessing and managing future and emerging risk by developing the results of the Emerging and Future Risk (EFR) method study into an emerging and future risk assessment lifecycle.

This is to include:

- Identification of additional elements missing in the EFR method, and are required in order to develop a workflow that supports scenario generation, validation and risk assessment
- Consideration of the issues and criteria which have been identified to influence the existence of risks, such as convergence, technology, applications and market trends as well as social and human behavioural factors
- Further consideration of effective risk assessment and criteria for the management of information security risks in relation of emerging and future scenarios
- Identification of criteria and constraints related to the development of the workflow
- Creation of the workflow for the lifecycle of the risk assessment and management of emerging and future risk including: scenario generation, validation of these scenarios, risk assessment and management, processing and quality assurance; taking into account any additional elements identified in the first bullet point above, and any criteria and constraints identified in the 4th bullet point above
- The presentation of the workflow in such a way that it can be translated into a set of automated electronic processes at an operational level, showing where possible how such translation could be conducted

The terminology used in the report should be in line with the international security standards – ISO 17799, ISO 13335, Common Criteria, BSI Standards and COBIT as well as the ENISA RM/RA Glossary.

1.2 EFR Process

This report introduces the EFR Process model that resulted from further development of the Methods for the identification of Emerging and Future Risks¹. It describes the approach taken to develop the processes and documents in outline the processes themselves. The process models are self documented and can be downloaded from http://www.enisa.europa.eu/rmra/er_downloads.html.

1.3 Structure of this document

The next section, Section 2 outlines the approach taken to develop the EFR Processes. Section 3 introduces the key processes added to existing risk assessment/risk management processes, together with an explanation of the organisational roles and the icons used to describe the processes.

This report provides a high level overview of the EFR process model, and it is emphasised that the process model¹ should be referred to whilst reading this report.

¹ Available from http://www.enisa.europa.eu/rmra/er_downloads.html

2 Development Approach

This section describes the approach taken in order to develop the EFR Processes.

2.1 Phase 1

The first phase completed the knowledge capture required to inform the development of the workflow. It ensured a complete understanding of ENISA's vision for emerging and future risk assessment, and how it integrates into ENISA's other processes.

Initially, the project team studied the approach taken by ENISA in fulfilling Article 3 (a) of Regulation 2004/460 – the collection of appropriate information in order to analyse current and emerging risks, as well as the formal references provided in the Technical Description of the Invitation to Tender on the processes regarding the collection and dissemination of emerging risk related information. The information collation method, security and privacy requirements in relation to ENISA and their stakeholders, and storage of information were all studied to define an architectural overview of a system² within which information pertaining to emerging and future risk is shared, stored and utilised for scenario generation and validation, and risk assessment and management.

Secondly, within this phase, the project team studied the architectural overview of the system and identified additional/missing elements of the required Emerging and Future Risk (EFR) method to develop a workflow through which information can be obtained and/or input from the relevant sources on demand, and used to generate and validate emerging and future scenarios which can then be analysed for vulnerabilities and potential threat agents. This took into account the issues and criteria which have been identified to influence the existence of risks, such as convergence, technology, applications and market trends as well as social and human behavioural factors in relation to the architectural overview of the system; as well as the wider context of the EFR method, based on the initial study into information collation and previous discussion with ENISA. This is illustrated below in Figure 1.

Workflow Management involves two main elements:

- a) setting up and configuring the workflow in order to integrate the chosen risk assessment and risk management approaches;
- b) validation of the EFR process and ongoing improvement activities.

Information Management includes the lifecycle of information; from collection to dissemination, including reception of requests and awareness.

Emerging and Future Risk comprises the structuring of scenarios and their validation.

RM/RA Method comprises the application of the preferred risk assessment and risk treatment methods.

In previous discussions with ENISA, we recognised that ENISA will build a repository of knowledge which will provide input to the EFR assessment, but 'filtered' according to who will be undertaking the EFR assessment. ENISA will have full access to their repository, but other external users may only have access to knowledge ENISA is able to make public. Also, it is recognised that the EFR method must be able to provide feedback as to the quality, completeness and currency of the knowledgebase users have access to. The ability to provide feedback will be part of the EFR assessment method, but taking action to improve and maintain the knowledgebase is not.

Once the identification of additional/missing elements within the EFR method to facilitate the workflow was agreed by ENISA, the contracted team members worked closely with

² System – a collection of components organised to accomplish a specific function or set of functions (IEEE 610)

ENISA to develop the criteria and constraints for the development of the workflow. On agreement of these criteria, and within the defined constraints, the team developed the workflow using the steps as described below.

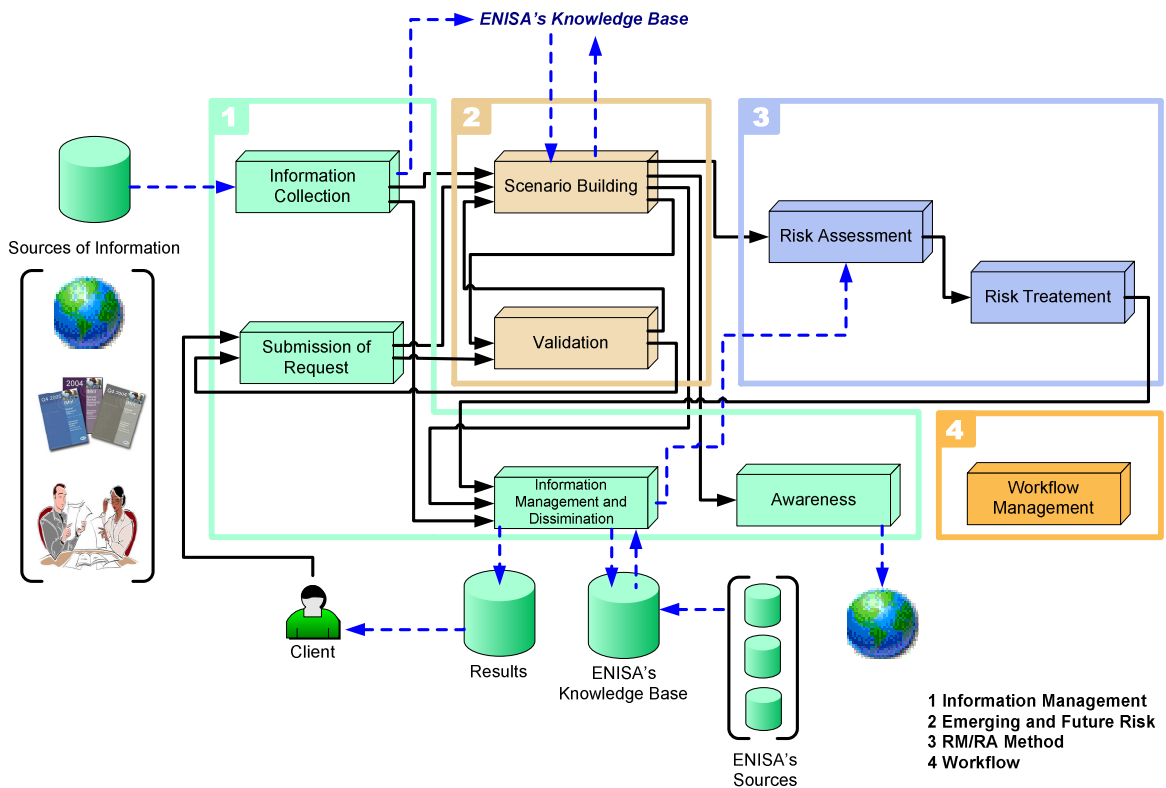


Figure 1 - System Overview

2.2 Phase 2

This phase began with an analysis of the Consensus Primary Task Model (CPTM) produced to develop the EFR method in order to understand what role would undertake each activity, what the inputs and outputs are, what the quality criteria are for the successful completion of the activity and what the information needs are. This is illustrated in Annex A.

We developed these roles by analysing the activities and determining which role is **A**ccountable for the activity being successfully completed, which roles are **R**esponsible for its completion, which roles are **C**onsulted in the progress of the activity and with roles are **I**nformed of the result. This is also called a RACI analysis and is illustrated in Annex B. Also, by considering each activity, we identified the information support needed.

Having completed the analysis of the activities, we considered the relevant standards and other best practice guidance to ensure all activities required for EFR assessment are understood. This added detail to the activities analysed previously. We also included the knowledge gained in the first phase regarding ENISA's specific needs. From this we built candidate process models using ADOit®, customising ADOit® where necessary to represent the desired workflow correctly.

The relationships between the activities in the CPTM informed the initial structure, but this was developed as we built the processes. The difference between the activities in the

CPTM and the process steps is that the CPTM activities state ‘what’ should be done, and the process diagram shows ‘how’ things should be done.

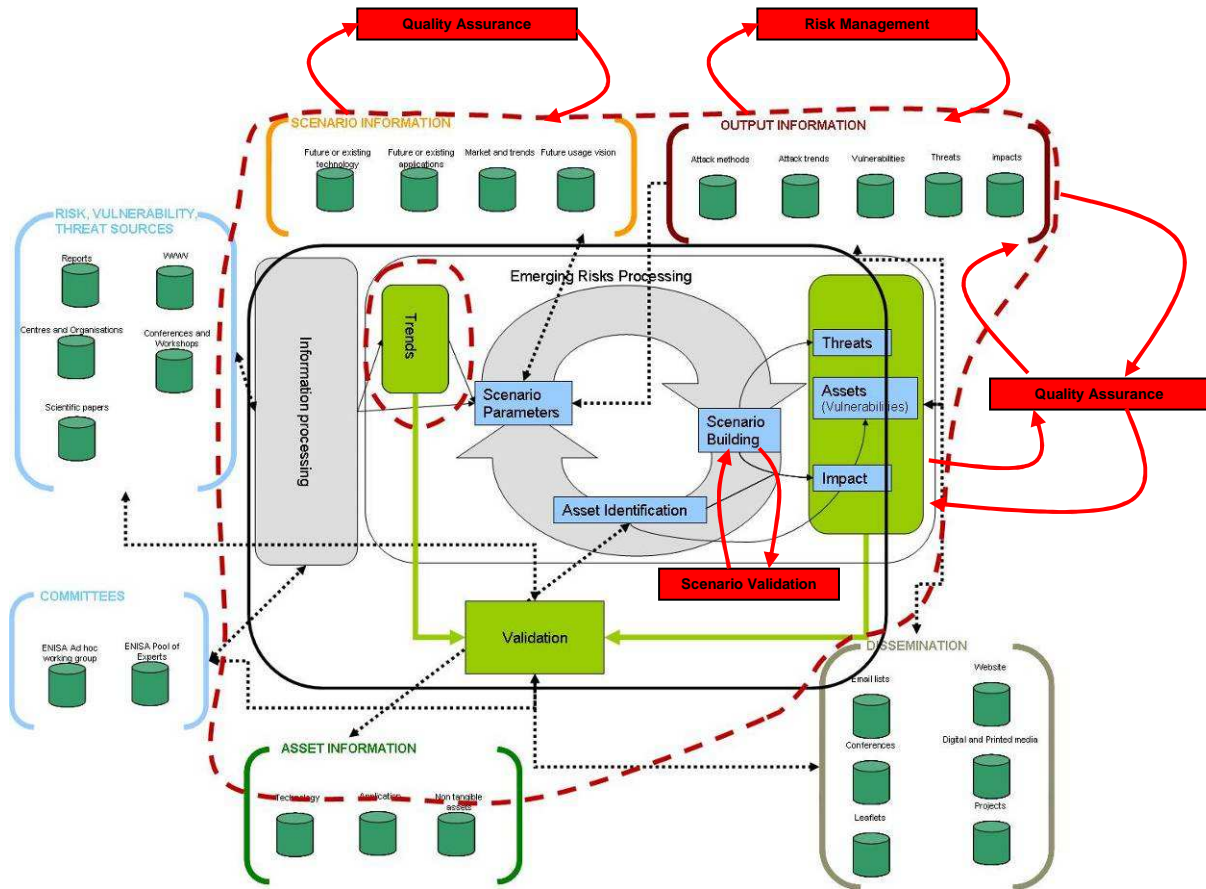


Figure 2 - Modified ENISA Model of EFR Method

Finally, we considered how the workflow relates to the ENISA model of the EFR method and supporting entities (Figure 3). Our additions to the diagram are shown in red where the scope of the EFR assessment method is denoted by the red dashed line. The scenario generation process is already present in the emerging risks lifecycle (labelled Scenario Building). We added a Scenario Validation step within the same lifecycle to impose a reality check on the generated scenario before taking it to the risk assessment stage. Likewise, in addition to the risk assessment module, we added a Risk Management module based on the outcome of the risk assessment, and a separate Quality Assurance module that evaluates and monitors the accuracy of the emerging and future risk information used to build scenarios, and the effectiveness of risk detection and management. The results of which will be fed back to the relevant people with the aim of creating an ongoing evaluation and improvement loop creating a more accurate and effective process model for the management of emerging and future risks.

2.3 Phase 3

The presentation of the workflow utilised the process modelling tool, ADONIS ADOit®.

3 Process Model

3.1 The EFR Lifecycle

The starting point for developing the EFR Process was the study on the Methods for the identification of Emerging and Future Risks (Requirements); as can be seen in the Figure 3 below, Scenario Acquisition, Scenario Generation and Scenario Validation are identified as the additional modules necessary in order to create an EFR lifecycle.

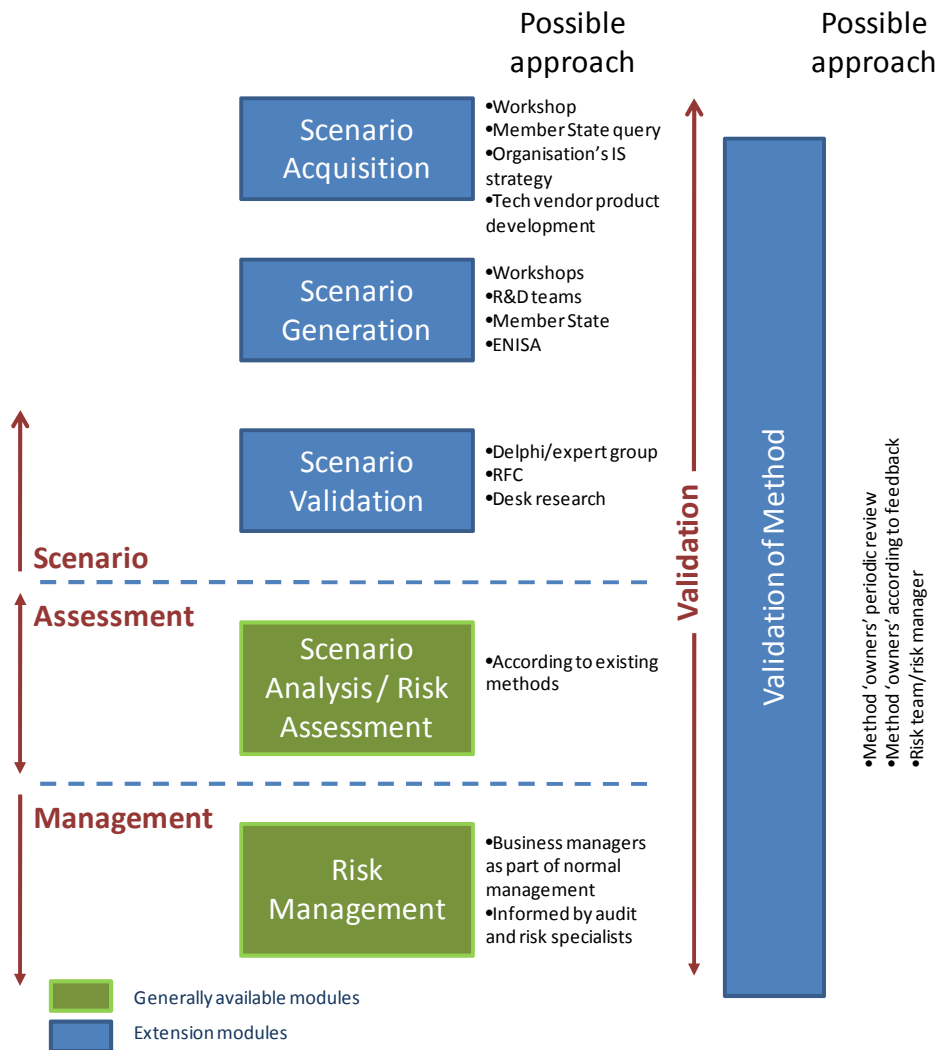


Figure 3 - Proposed EFR Lifecycle

3.2 The EFR process model

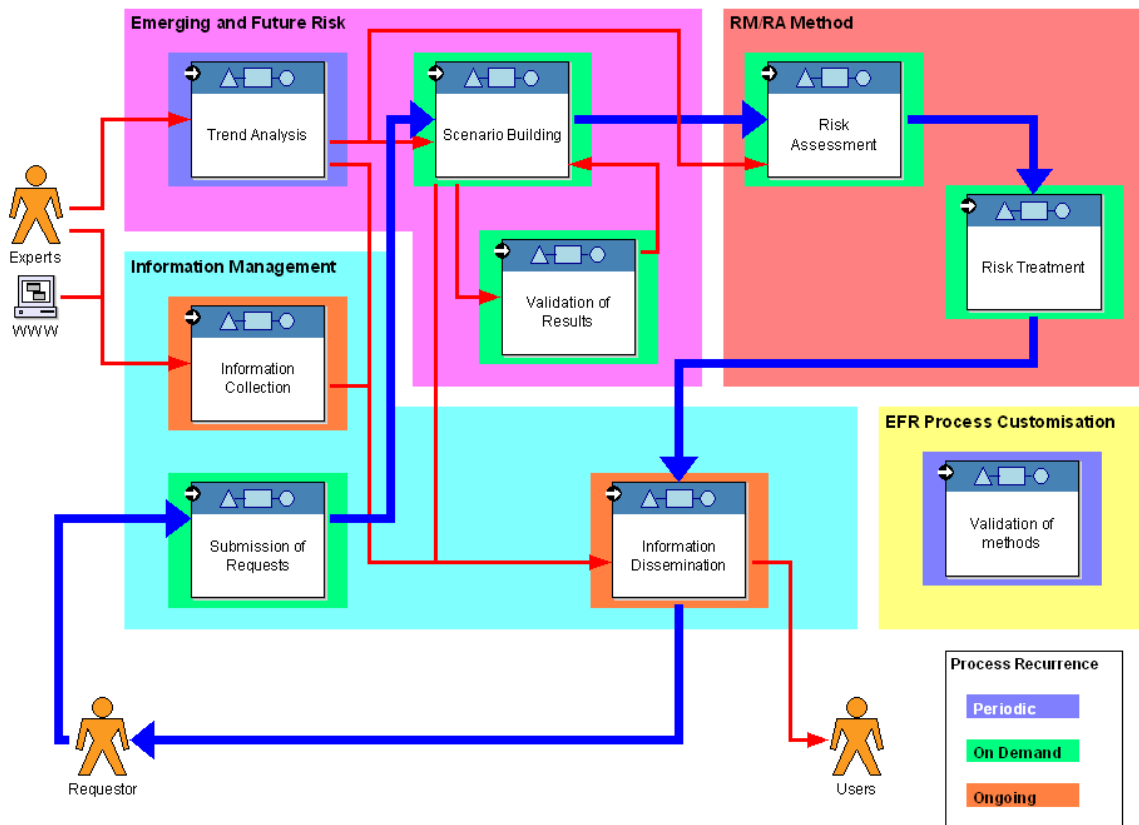


Figure 4 - Top-level Process Model

In order to facilitate the execution of the EFR lifecycle, a detailed process model was developed to provide guidance on the tasks and activities to be undertaken, information support requirements and the corresponding roles and responsibilities. The above diagram (Figure 4), developed in ADOit®, illustrates the key process flow (in blue) and the top level processes that constitute the EFR lifecycle. In this process model, requests are 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;
- EC, consumer organisations, non-governmental organisations (NGOs) etc considering the impact of strategic IS/IT planning or considering the development/implementation of new and innovative applications or technology.

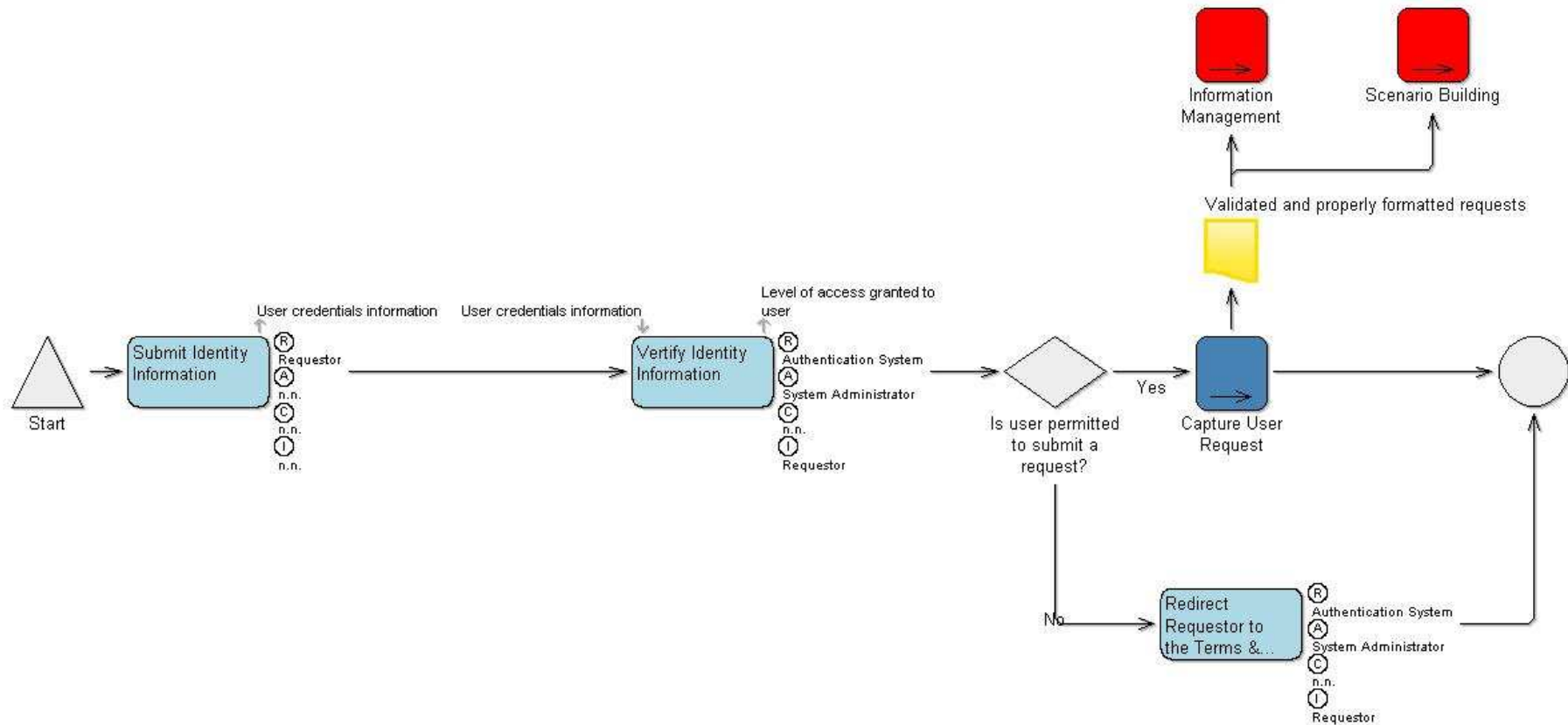
The resulting scenarios would be developed and validated by subject matter experts and take into account current knowledge gleaned from various sources including the World-Wide Web, white papers and research papers. Trend analysis would also be commissioned periodically and the impact applied both to scenarios being developed, and on scenarios stored.

Sections 3.2.2, 3.2.3 and 3.2.7 contain diagrams of the Scenario Building, Scenario Validation and Validation of Methods processes, whilst Annex B illustrates the roles included within the full set of processes.

It should be noted that a full set of process diagrams in html format may be obtained from the ENISA RMRA website http://www.enisa.europa.eu/rmra/er_downloads.html and should be referred to whilst reading this report.

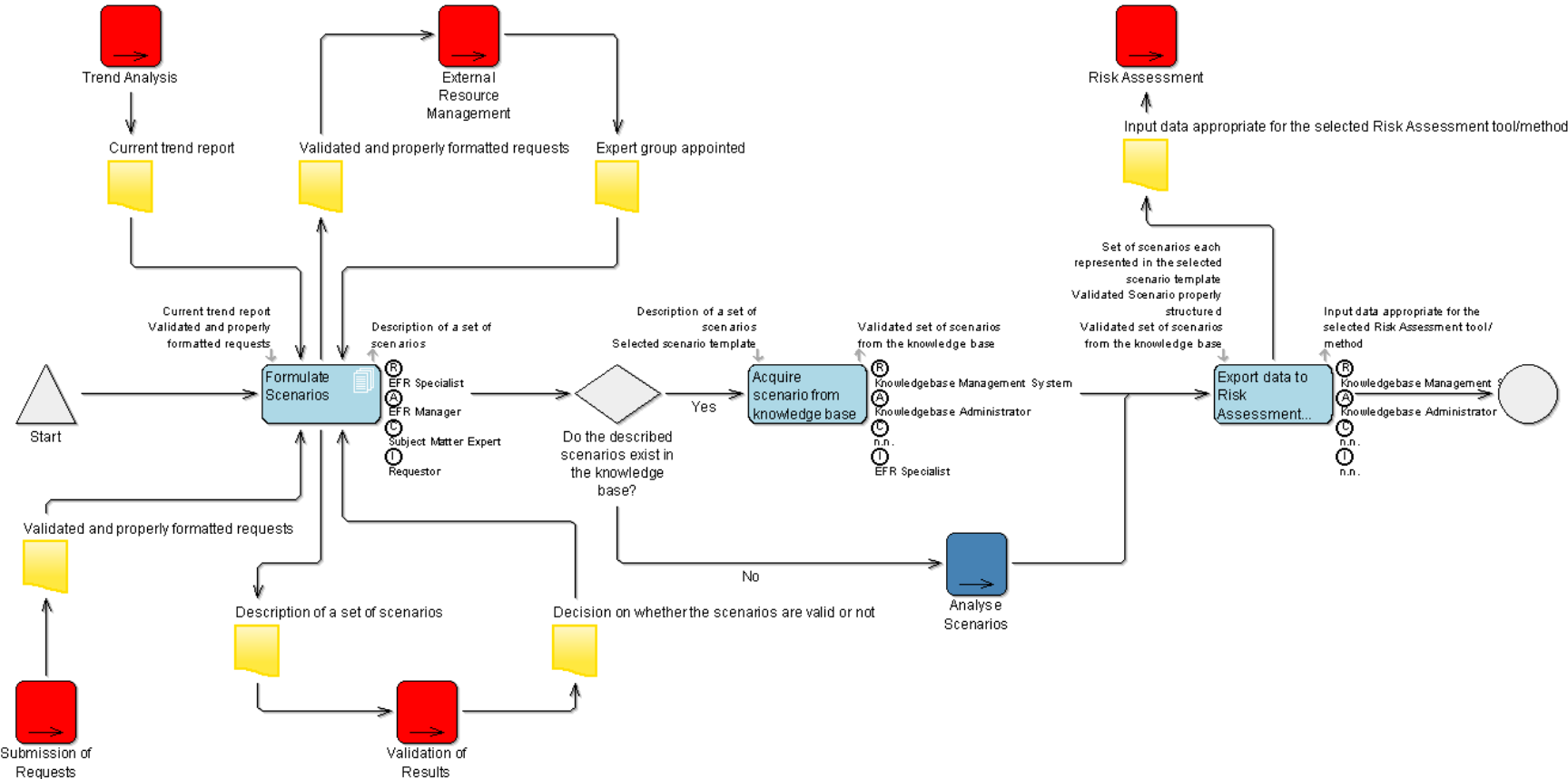
3.2.1 Submission of Requests

Users interested in assessing emerging and future risks that may arise from the implementation of specific combinations of new or existing technologies with new or existing applications submit a request to ENISA through this process. Proper authentication is required to establish whether the requestor is permitted to submit request. The submitted request includes the user's specific requirements properly formatted to be used in the scenario building process.



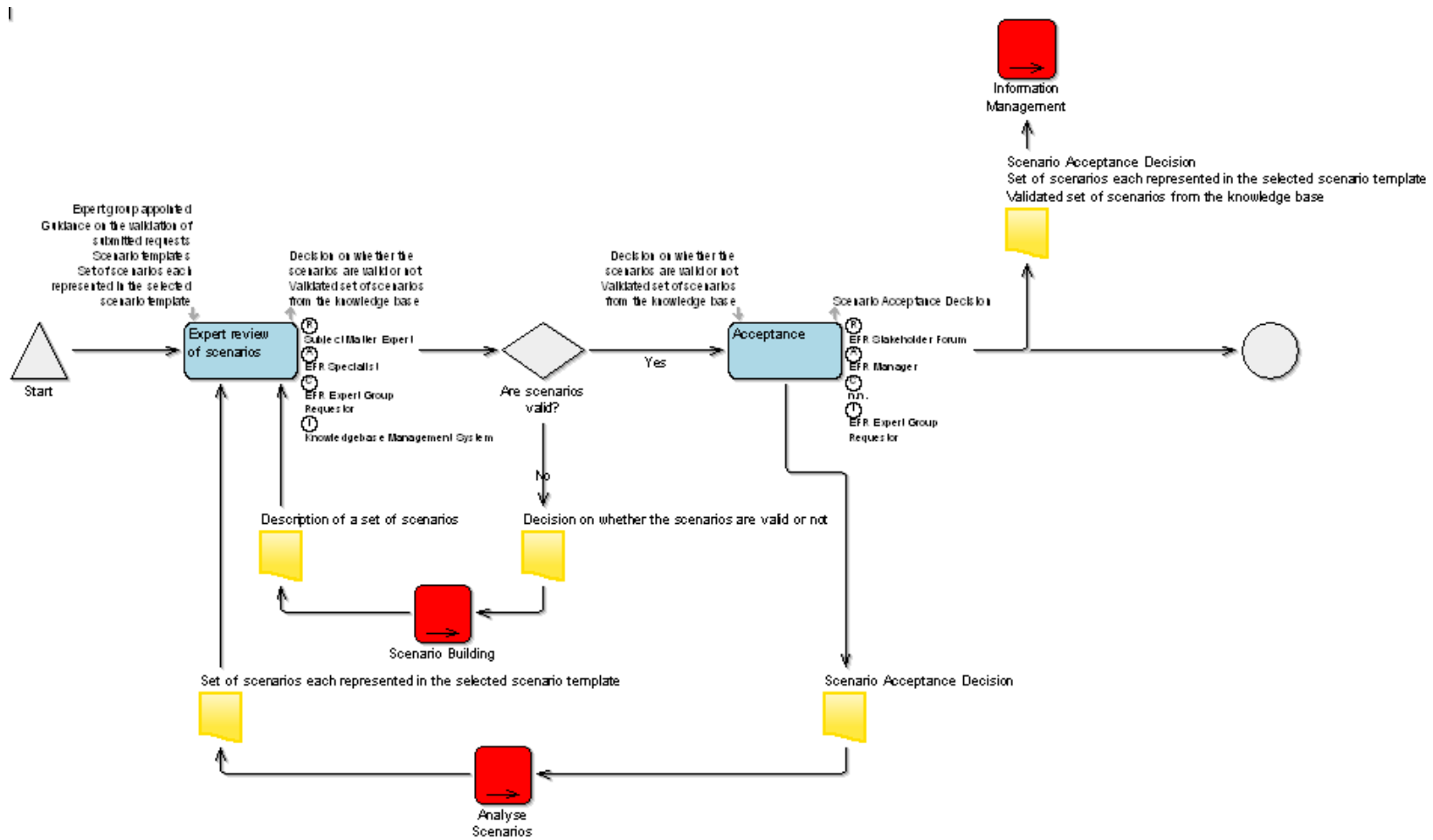
3.2.2 Scenario Building

In this process, relevant usage scenarios based on the specific requirements defined by the requestor are formulated and analysed. The generated scenarios are stored in the knowledge base for future reference and evaluation, and scenario details are also exported to the chosen risk assessment method. This process utilised the expert knowledge of subject matter experts, in addition to the outcomes of the trend analysis process, to achieve its purpose in generating relevant and useful scenarios that could be exploited to conduct risk assessment.



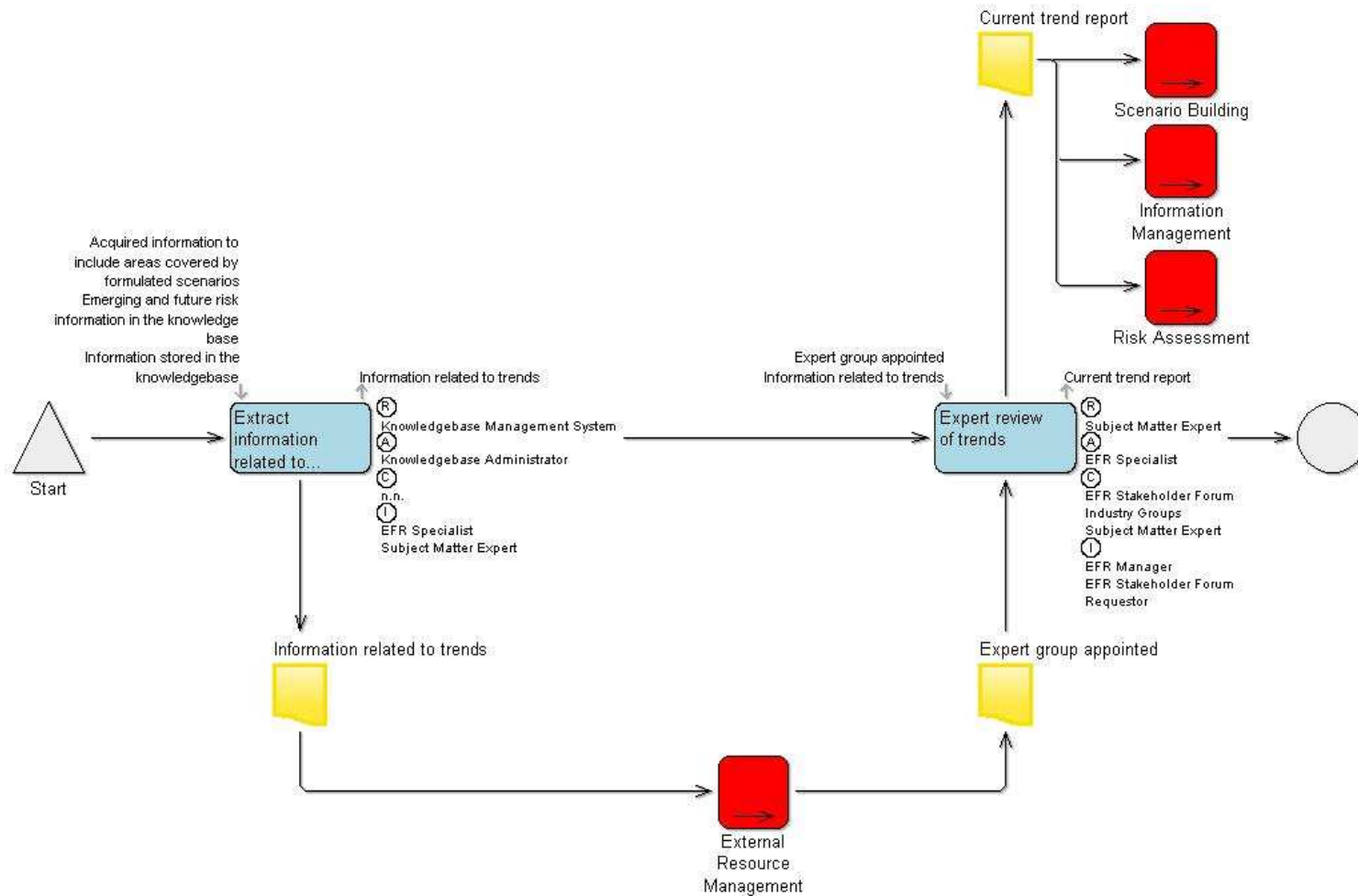
3.2.3 Validation of Results

The purpose of this process is to ensure that the generated scenarios are valid and useful for the risk assessment exercise. Experts will review the generated scenarios and make appropriate decisions on their validity. If valid, the generated scenarios are then accepted by the EFR Stakeholder Forum. Otherwise, the scenarios may need to be reworked again.



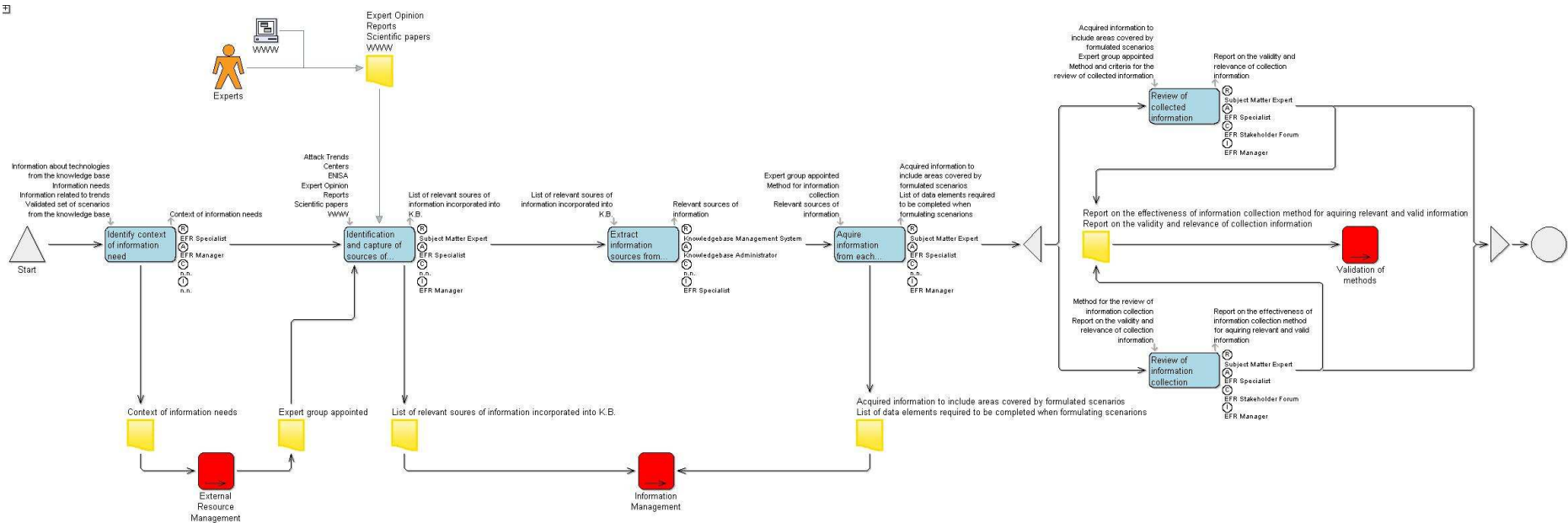
3.2.4 Trend Analysis

This process aims to support the scenario building process by identifying, reviewing and documenting relevant trends from the risk and scenario information previously identified and stored in the knowledgebase.



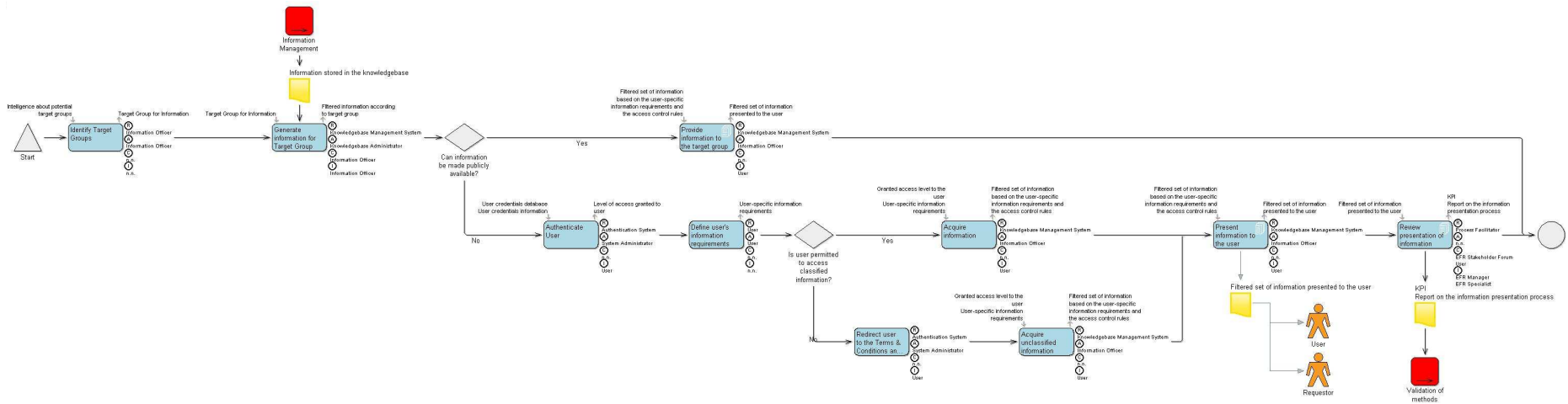
3.2.5 Information Collection

The activities in this process are primarily concerned with the identification of information needs to support the EFR process, the identification of relevant sources of information to satisfy these needs and the acquisition and review of required information. Expert knowledge is utilised to guide the information acquisition and review activities. Acquired information is then properly formatted, indexed, classified and stored in the knowledgebase.



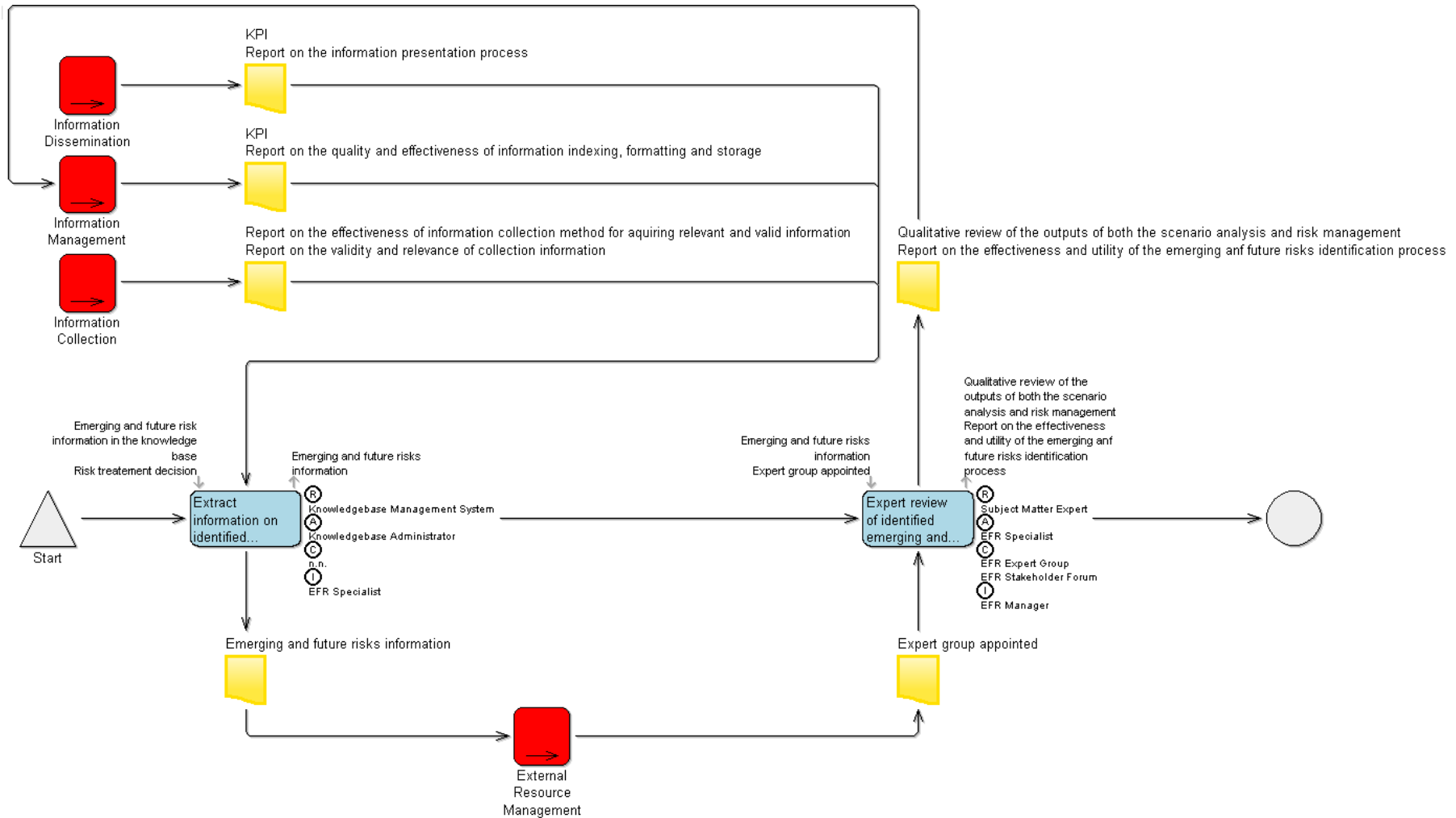
3.2.6 Information Dissemination

This process provides the interface between the EFR knowledgebase developed by ENISA and its target audience. It contains activities 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.



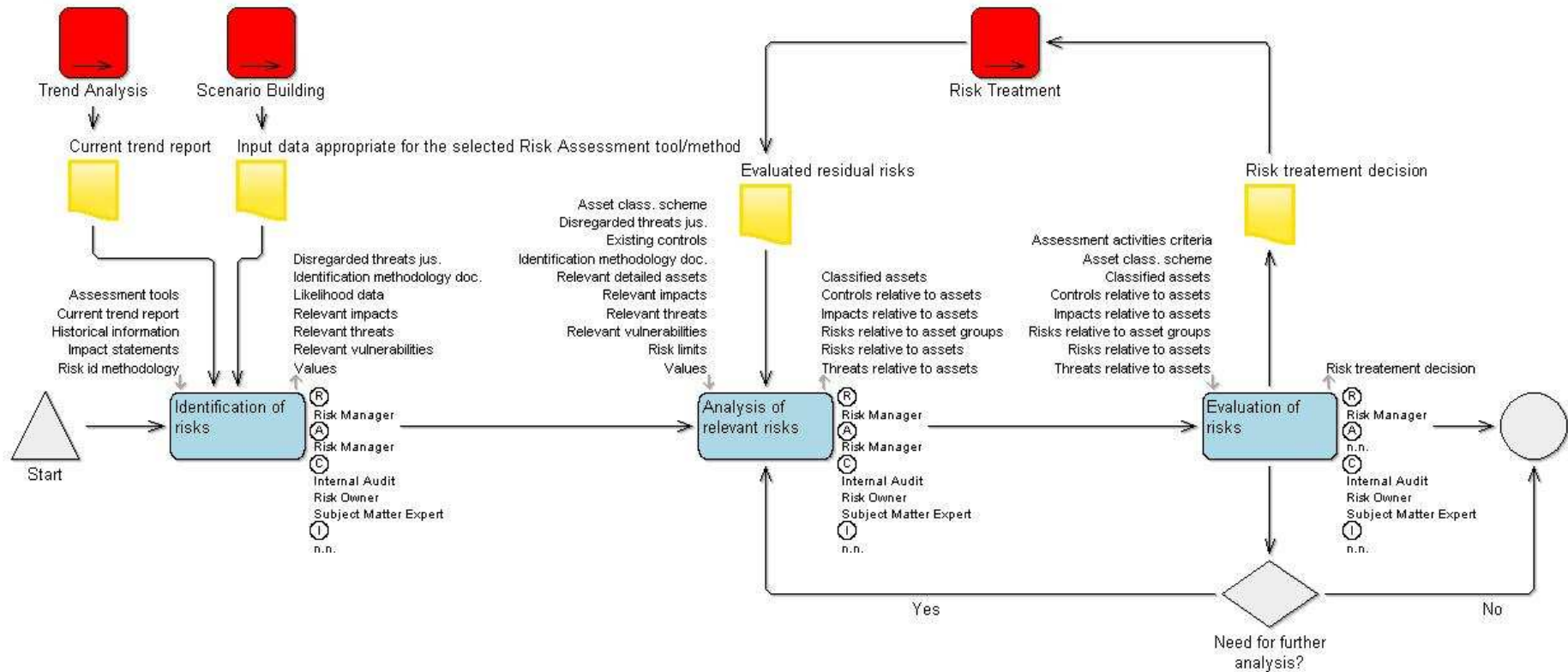
3.2.7 Validation of Methods

Improvement of the EFR process is achieved through the continuous validation of the methods utilised in analysing scenarios and assessing and managing risks. The validations results provide the opportunity to improve the process by altering or changing the adopted methods.



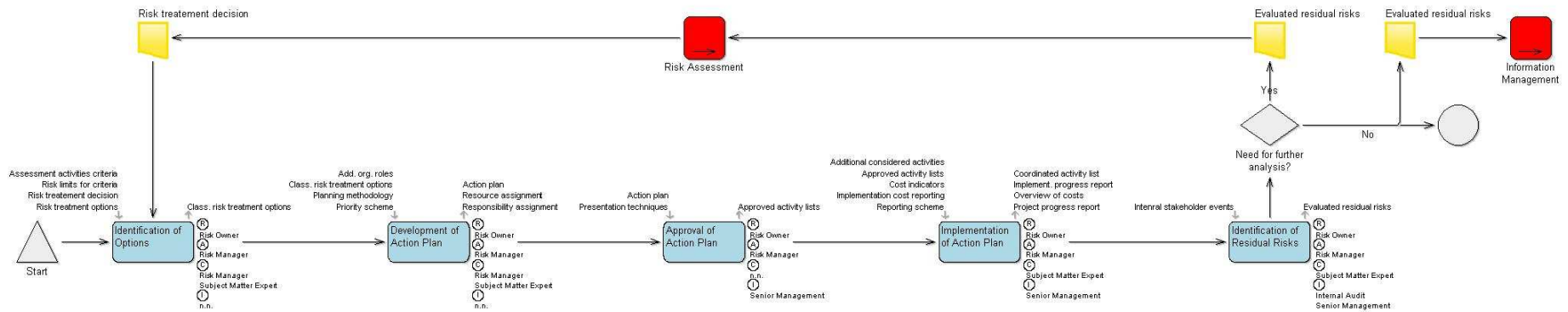
3.2.8 Risk Assessment

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 the threats, vulnerabilities and impacts relevant to each scenario in order to analyse potential risks. Appropriate risk treatment decisions are then produced based on the evaluation of these risks.



3.2.9 Risk Treatment

While the risk assessment process 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.



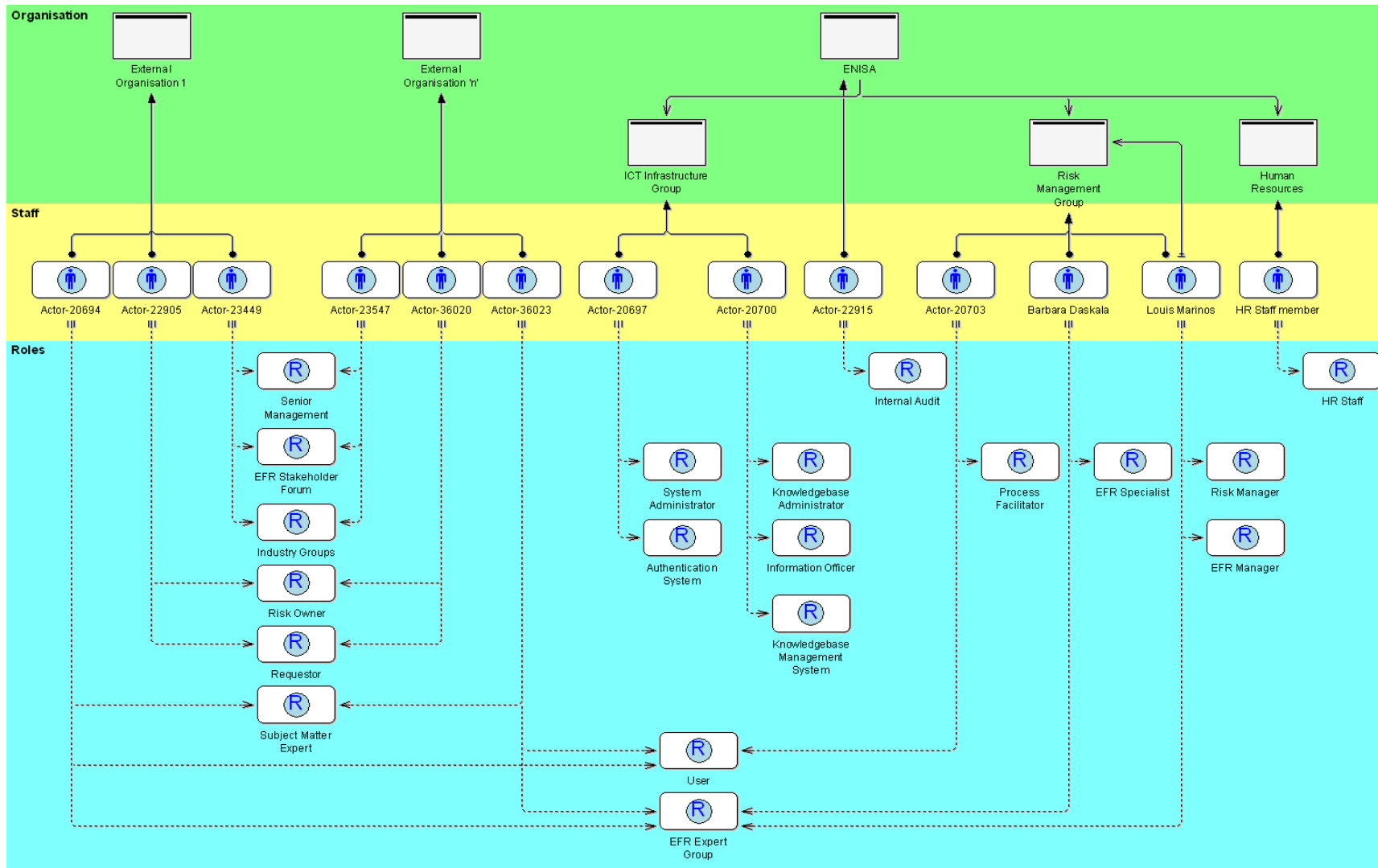
3.3 Organisational Roles

The following set of roles have been identified:

- **User/Requestor:** users submit requests for the identification and assessment of emerging and future risks relevant to a combination of existing/new technology with an existing/new application that matches their own requirements. They are also provided with the risk identification and assessment results for these requirements. Users' identification and interaction with the system is facilitated through the authentication system.
- **Process Facilitator:** ensures the smooth operation and quality of the EFR process by reviewing and evaluating relevant aspects of the process operation.
- **EFR Specialist:** primarily concerned with the risk related aspects of the EFR process. The EFR specialist 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.
- **Risk Manager:** oversees the risk identification and assessment process to ensure its effective and successful operation.
- **EFR Manager:** supervises the actions of the EFR specialist and is accountable for the successful identification of the context of information needs and classification of risk related information.
- **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. This role is typically recruited for particular assignments.
- **Information Officer:** is concerned with the information dissemination aspects of the EFR process, including the identification of target groups, support for the generation of information for these target groups and presentation of information to users.
- **HR Staff:** responsible for ensuring the availability of required Subject Matter Experts and other personnel to undertakes the tasks and activities included in the EFR process.
- **Internal Audit:** undertakes required audit operations to evaluate the effectiveness of the EFR in achieving its objectives.
- **Authentication System:** is responsible for the identification of users, verification of users' credentials and establishing the appropriate access level granted to each user.
- **System administrator:** undertakes all activities and tasks required to ensure the continuous and correct operation of the authentication system and other automated systems.
- **Knowledgebase Management System:** performs all the operations related to information processing, indexing, storage, retrieval and dissemination. This includes scenario templates, emerging and future risk information, requests submitted by users, etc.
- **Knowledge Administrator:** undertakes all activities and tasks required to ensure the continuous and correct operation of the knowledgebase management system.

- **EFR Stakeholder Forum:** reviews and accepts the generated EFR scenarios, and is consulted in risk related tasks and activities.
- **Industry Groups:** are consulted in the review of trends.
- **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, implement action plans and evaluate residual risks. It is also consulted in the identification, analysis and evaluation of risks.
- **Senior Management:** of the entity that is directly affected by the existence of risks. The risk owner should inform its senior management of the approval and implementation of risk treatment plans and the identification of residual risks.

These roles have been appropriately incorporated into the EFR workflow, as depicted in the following image, taken from the ADOit Model..



Annex A Activity Analysis

Below is an extract from the scenario analysis undertaken for the whole model created in the Methods for the identification of Emerging and Future Risks (Requirements) report:

Task ID	Task	Task Purpose	Encompassed Activities	Activity ID	Activity	Input	Preceding Activities	Output	Succeeding Activities	Quality Criteria
Tasks			Activities			Scenario Building				
Updated by Anas on 30.01.08										
T.1	Decide on an approach/methodology for generating future scenarios	To clarify exactly how future scenario generation should occur	A.11	A.11	Identify possible ways of generating future scenarios	Definition of future scenario	A.10	Possible methods/approaches to future scenario generation	A.12	Usefulness Applicability
T.2	Decide how to apply information from knowledge base related to new and existing technologies, and developments in technology into scenario generation	To utilise information sourced into a knowledge base in the most effective way	A.9, A.7, E.12	A.9	Decide on how to apply new technology to existing applications	Knowledge base of new technologies	A.8	Potential ways of applying new technology in existing applications	A.13	Expert Advice
				A.7	Decide on how to apply existing technologies in forthcoming application scenarios	Knowledge base of existing technologies	A.6	Potential for using existing technology in future scenarios	A.13	Expert Advice Match to Technology Trends
				E.12	Decide on how to make use of relevant developments in technology	Updates of relevant developments in technology incorporated in the knowledge base Opinions on how the developments in technology can be exploited	E.10	Plan for exploiting relevant developments in technology	E.13	Relevance Expert Advice Feasibility
T.3	Build scenario detail	To structure and present the detail of a scenario	A.28	E.15	Assess use of relevant developments in technology	Report on the exploitation of relevant developments in technology	E.14	Analysis of report assessing exploitation of relevant developments in technology	E.17	Objectivity Coverage Expert Advice
				A.28	Generate future scenarios	Method for generating future scenarios detailing information requirements, methods for information collection, and process for deriving scenarios List of accepted sources of information	A.13 A.18	Detailed future scenarios	A.29 A.33	Expert advice Completeness

The task is identified in the Model Relevant to Emerging Risks Methods found at Annex C to the Methods for the identification of Emerging and Future Risks (Requirements) report. From these, relevant activities were determined and analysed, thereby identifying the inputs and outputs. Identifying the preceding and succeeding activities laid the foundation for the processes.

Annex B Role Analysis

A RACI table was developed as illustrated below by listing the activities and defining roles necessary to carry out the activities: 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.

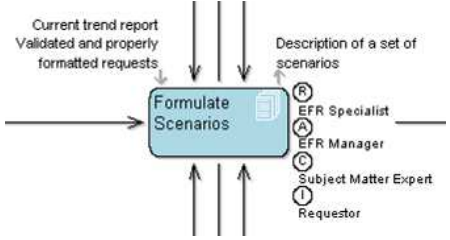
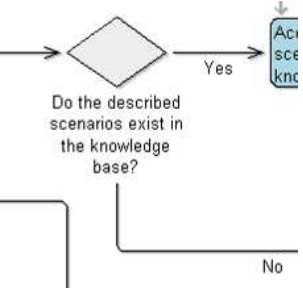
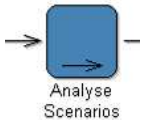


Tabulating the analysis enables consistency of roles which is not easy if you only have the RACI recorded within the processes.

Considering a horizontal view of the table enables an understanding of the RACI relevant to the activities, whereas a vertical Role-based view enables the development of job descriptions and role skills and experience profiles.

	Requestor	Process Facilitator	EFR Specialist	Subject Matter Expert	System Administrator	Knowledge Base Administ	Authentication System	Knowledge Base Mgmt S	ERR Manager	Information Officer	EFR Expert Group	EFR Stakeholder Forum	Risk Manager	Risk Owner	Internal Audit	Industry Groups	Senior Management	Human Resources	
Submission of Requests																			
1	Submit Identity Information	R																	
2	Verify Identity Information	I			A		R												
3	Redirect Requestor to the Terms & Conditions	I			A		R												
4	Obtain template for submission of request from knowledge base					A		R											
5	Present user with a template for the submission of request					A		R											
6	Submission of completed template	R							A										
7	Validation of submitted request		A					R											
Scenario Building																			
1	Formulate Scenarios	I		R	C				A										
2	Acquire scenario from knowledge base			I			A	R											
3	Export data to Risk Assessment method/tool					A		R											
4	Select scenario template	I		R	C				A										
5	Analyse Request			R					A, I										
6	Check Technology			I		A		R											
7	Check Application			I		A		R											
8	Acquire information on relevant new applications			I		A		R											
9	Acquire information on relevant existing or new applications			I		A		R											
10	Acquire information on relevant new technologies			I		A		R											
11	Acquire information on relevant existing or new technologies			I		A		R											
12	Identify actors			A	R			I											
13	Identify devices			A	R			I											
14	Determine activities undertaken			A	R			I											
15	Populate scenario template			A	R			I											
16	Expert review of scenarios	C		A	R			I											
17	Acceptance	I							A		I	R							
Risk Assessment																			
1	Identification of risks				C									R, A	C	C			
2	Analysis of relevant risks				C									R, A	C	C			
3	Evaluation of risks				C									R, A	C	C			
Risk Treatment																			
1	Identification of Options				C									A, C	R				
2	Development of Action Plan				C									A, C	R				
3	Approval of Action Plan													A	R				I
4	Implementation of Action Plan				C									A	R				I
5	Identification of Residual Risks				C									A	R	I			I
Information Collection																			
1	Identify context of information need			R				A											
2	Identification and capture of sources of information			A	R			I											
3	Extract information sources from K.B.			I		A		R											
4	Acquire information from each source			A	R			I											
5	Review of collected information			A	R			I		C									
6	Review of information collection			A	R			I		C									
Information Dissemination																			
1	Identify Target Groups									R, A									
2	Generate information for Target Group					A		R		C, I									
3	Provide information to the target group	I						R		A									
4	Authenticate User	I			A		R												
5	Define user's information requirements	R, A																	
6	Acquire information	I						R	A										
7	Present information to the user	I						R	A										
8	Review presentation of information	C	R	I					I		C								
9	Redirect user to the Terms & Conditions and the public website	I			A		R												
10	Acquire unclassified information	I					R	A											
Information Management																			
1	Index and formation information			I		A		R											
2	Information Storage			I		A		R											
3	Classify Information			R				I											
4	Review information indexing, formatting and storage	R, A	I					I											
External Resource Management																			
1	Identify skills required of experts for each scenario			R				A											
2	Select and appoint experts			I	I			A											R
Trend Analysis																			
1	Extract information related to desired trend consideration			I		A		R		I									
2	Select and appoint experts	I		A	R, C			I		C, I									C
Validation of methods																			
1	Extract information on identified emerging and future risks			I		A		R											
2	Expert review of identified emerging and future risks			A	R			I		C	C								

Annex C Icons used within Processes

The icons used within the detailed processes are described in the table below.

Icon	Description	Icon	Description
 <p>The icon shows a central blue rounded rectangle labeled 'Formulate Scenarios'. To its left, an arrow points from the text 'Validated and properly formatted requests'. Above the box, three vertical arrows point down from the text 'Current trend report'. To the right, three vertical arrows point up from the text 'Description of a set of scenarios'. To the right of the box, four roles are listed with corresponding icons: 'EFR Specialist' (R), 'EFR Manager' (A), 'Subject Matter Expert' (C), and 'Requestor' (I).</p>	<p>This icon is an activity within the process. The words on the top left of the process denotes inputs, and those on the top right of the process denotes outputs.</p> <p>To the right of the process is an indication of the roles Responsible for carrying out the activity, Accountable for ensuring the activity happens, Consulted in the progress of the activity, or Informed of the outcome.</p>	 <p>The icon is a diamond-shaped decision box containing the text 'Do the described scenarios exist in the knowledge base?'. An arrow enters from the left. Two arrows exit: one labeled 'Yes' pointing to a vertical bar icon labeled 'Acc kn', and one labeled 'No' pointing to the right.</p>	<p>This icon denotes a decision step with mutually exclusive outcomes.</p>
 <p>The icon is a blue rounded rectangle labeled 'Analyse Scenarios' with an arrow pointing into it from the left and another arrow pointing out to the right.</p>	<p>This icon denotes a nested process where the only occurrence of the process is nested within a higher level process.</p>	 <p>The icon is a red rounded rectangle labeled 'Trend Analysis' with an arrow pointing into it from the left.</p>	<p>This icon is an interface process and is included to link separate processes</p>
 <p>The icon is a yellow sticky note shape with the text 'Validated and properly formatted requests' written above it.</p>	<p>This icon refers to an information item exchanged between processes, with an associated description of the information exchanged.</p>		