

Emerging and Future Risks Executable Workflow UML Description

Conducted by the
Technical Department of ENISA
Section Risk Management

In cooperation with the:
VTT Technical Research Centre of Finland.

November 2008



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 contacting ENISA or for general enquiries on EFR Workflow, please use the following details:

Dr. Louis Marinos, Senior Expert Risk Management
Barbara Daskala, Expert Risk Management
e-mail: RiskMngt@enisa.europa.eu
Internet: <http://www.enisa.europa.eu/rmra/>

Document Revision: 1.0

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless 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 websites referenced in this publication.

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

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2008

Glossary

| Term | Explanation |
|----------------------|--|
| Action | Action is a smaller part than activity |
| Activity | Activity is a set of actions |
| EFR | Emerging and future risk |
| EFR Process Overview | Structured HTML presentation of the EFR process at a conceptual level |
| KB | Knowledgebase |
| RA / RT | Risk assessment / Risk treatment |
| SA | Scenario analysis |
| Scenario | Scenario is a specific case that may contain possible emerging and future risks. |

| Actor | Explanation |
|-----------------------|---|
| 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. |
| EFR Expert Group | ENISA selects this group from the EFR Stakeholder forum for reviewing and accepting generated EFR scenarios. |
| 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. |
| Requestor | Member States, EC, consumer organizations, non-governmental organisations, etc. Requestor submits 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. |
| 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. |
| User | User is a general description for a role that gets information in the information dissemination phase. |

1. Introduction

ENISA's tasks, as described in Regulation 460/2004¹, include the collection of appropriate information in order to analyse current and emerging risks. In 2006, ENISA provided an indicative roadmap² to address the issue of contemporary, emerging and future risk in risk management. In accordance with this roadmap, methods for the identification of emerging and future risks were investigated. Building on these ENISA has developed a workflow to perform an identification and analysis of emerging and future risks the "EFR Process Workflow"³. The EFR (Emerging and Future Risk) workflow is an approach to systemise and automate the treatment of emerging and future risks. This document provides a description of the scenario building and analysis phases of the EFR workflow as UML (Unified Modelling Language) activity diagrams. The data elements, the actions, and the roles of actors committing to them, as well as the EFR treatment's interface to risk management (the RA/RT phase) are described. Also, a data model is included, describing the used data elements and the primary relationships in between them. As such, the document can be used as a specification for the prototyping and subsequent implementation projects.

This document was prepared in cooperation with: Reijo Savola, Evesti Antti of VTT Technical Research Centre of Finland.

2. Design principles

The EFR system will be a client-server system, i.e. web-based desktop clients using a database on a server machine. The EFR workflow is based on the previous work of ENISA the "EFR Process Workflow".

The "EFR Process Workflow" is a process model that contains abstract definitions of activities, lists stakeholders and describes input and output data flows. Here, the workflow is specified in detail, defining each activity as a group of atomic actions, which all together implement the executable workflow. Thereby the activities presented in EFR Process Overview are divided up to the smaller actions, which have only one stakeholder and input and output data specified in detail.

The refined workflow is presented in UML using the Activity Diagram notation. Activity Diagram presents the system stakeholders, i.e. humans and automated systems, as swim-lanes (partitions). The swim-lane representation naturally carries the actor information of each activity, which benefits the future workflow prototyping. Activity Diagrams contain transitions

¹ 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, OJ L 77, 13 March 2004

² The contemporary and emerging risks roadmap (http://www.enisa.europa.eu/rmra/er_roadmap.html)

³ EFR Process Workflow (http://www.enisa.europa.eu/rmra/files/efr_process_model.zip)

between the actions. These transitions represent, for example, a control or an object flow. The control flow describes pure control transitions between the actions, whereas the object flow presents the transitions to deliver a specific data object. Both of these transition types are represented in the workflow. In Activity Diagrams a rounded rectangle depicts an activity, and a rectangle means a data object transmitted between the activities. Alternatively, specific data objects can be modelled as named squares attached to the related action element. The rather large workflow has been divided into readable chunks by using a hierarchy in the description of the activities: an activity with a spectacle symbol has a finer structure described as a separate diagram. The lowest level atomic activity elements are called actions.

Sparx systems' Enterprise Architect has been used as the UML tool in this specification. Enterprise Architect is compliant with OMG's (Object Management Group) UML 2.0 standard.

3. Workflow refinement

The workflow refinement is presented in this section as Activity Diagrams. The workflow is divided into four parts, namely *Root level*, *Submission of request*, *Scenario building and analysis* and *Information management*.

Root level of the EFR workflow

Figure 1 contains the main processes of the EFR workflow and the used input/output data objects of these processes. An arrow symbol depicts process and a class symbol with stereotype 'resource' represent flowing data object. The Information dissemination process is depicted separately without input data. However, each data object can act as an input for the Information dissemination, but these input arrows are not depicted because of clarity issues.

cd Process diagram

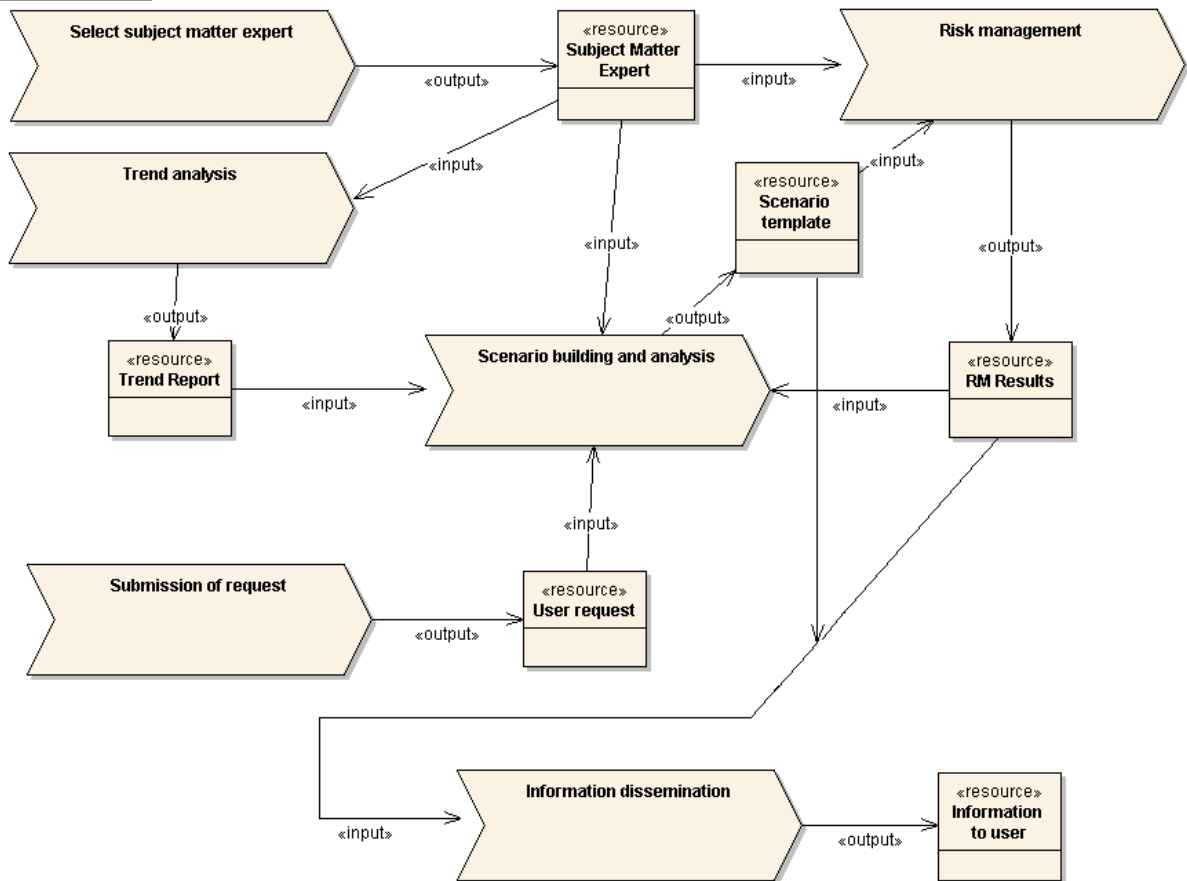


Figure 1 Root level process diagram of the EFR Workflow

Figure 2 represents a root level of the EFR Workflow, and the following sections give more detailed descriptions of the main activities visible here. After each Activity Diagram, there is a table that introduces the related data objects. Section 5 gives a compound description of the data objects.

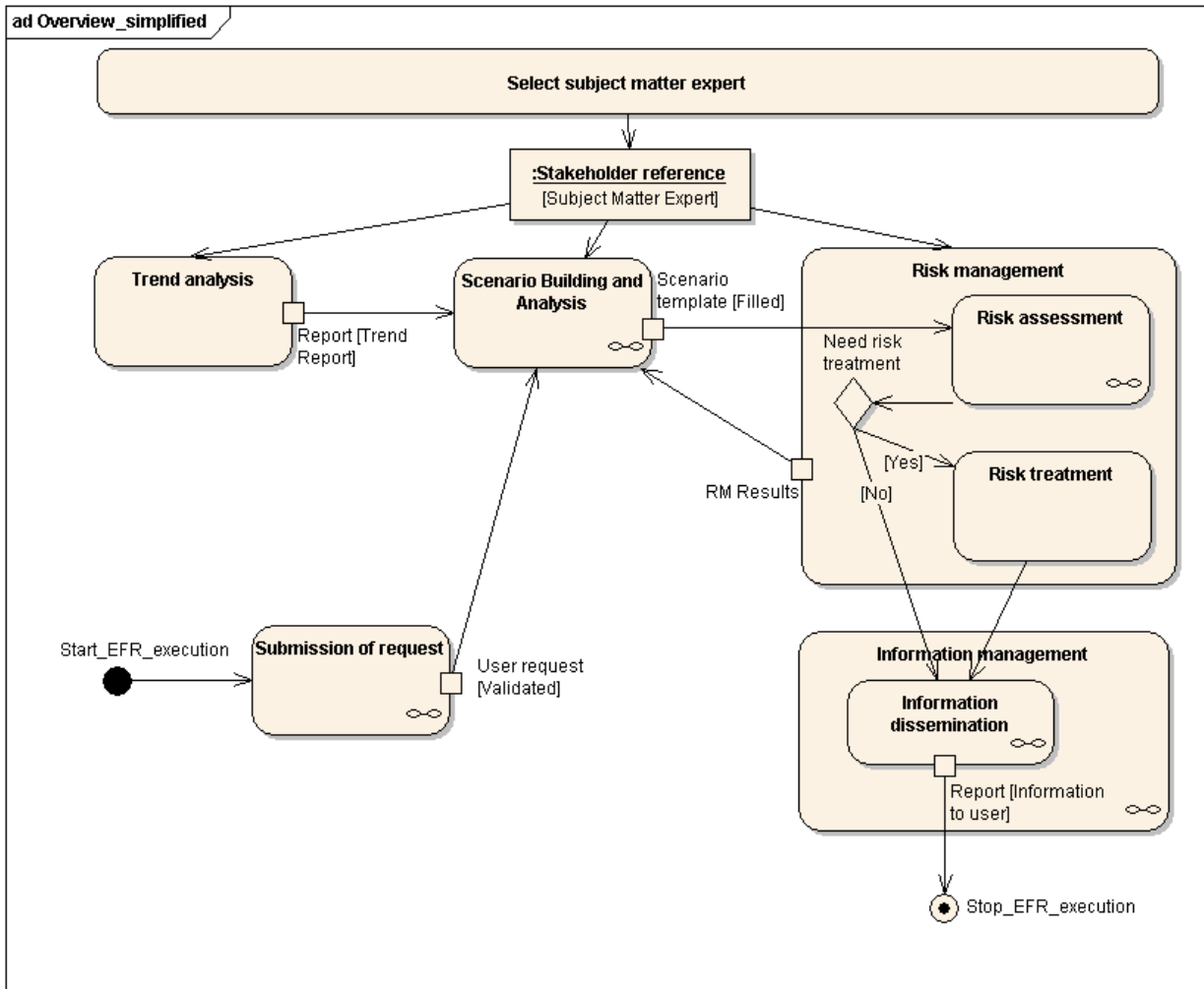


Figure 2 Root level activity diagram

| Used data objects in activity |
|---|
| Report [Trend report] |
| User request [Validated] |
| Scenario template [Filled] |
| Report [Information to user] |
| Stakeholder reference [Subject Matter Expert] |
| RM results |

In Figure 3, the same activities are described as in Figure 2, but now data object movements via the *Information management* activity are presented to the detail. This picture describes the importance of the *Information management* because all transmitted data objects are moved via it.

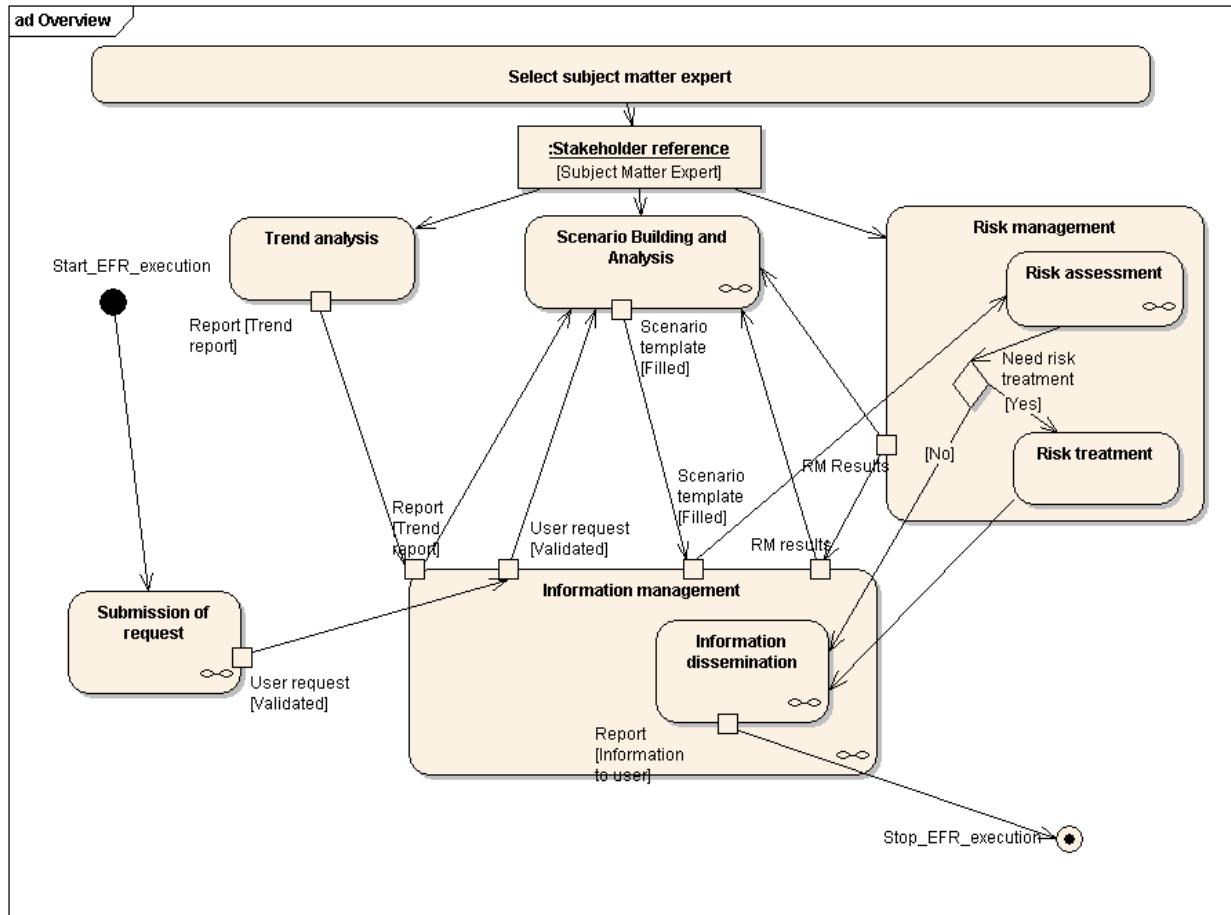


Figure 3 Detailed root level

Submission of requests

Figure 4 represents the *Submission of request* and Figure 5 refines its *Capture user request* activity.

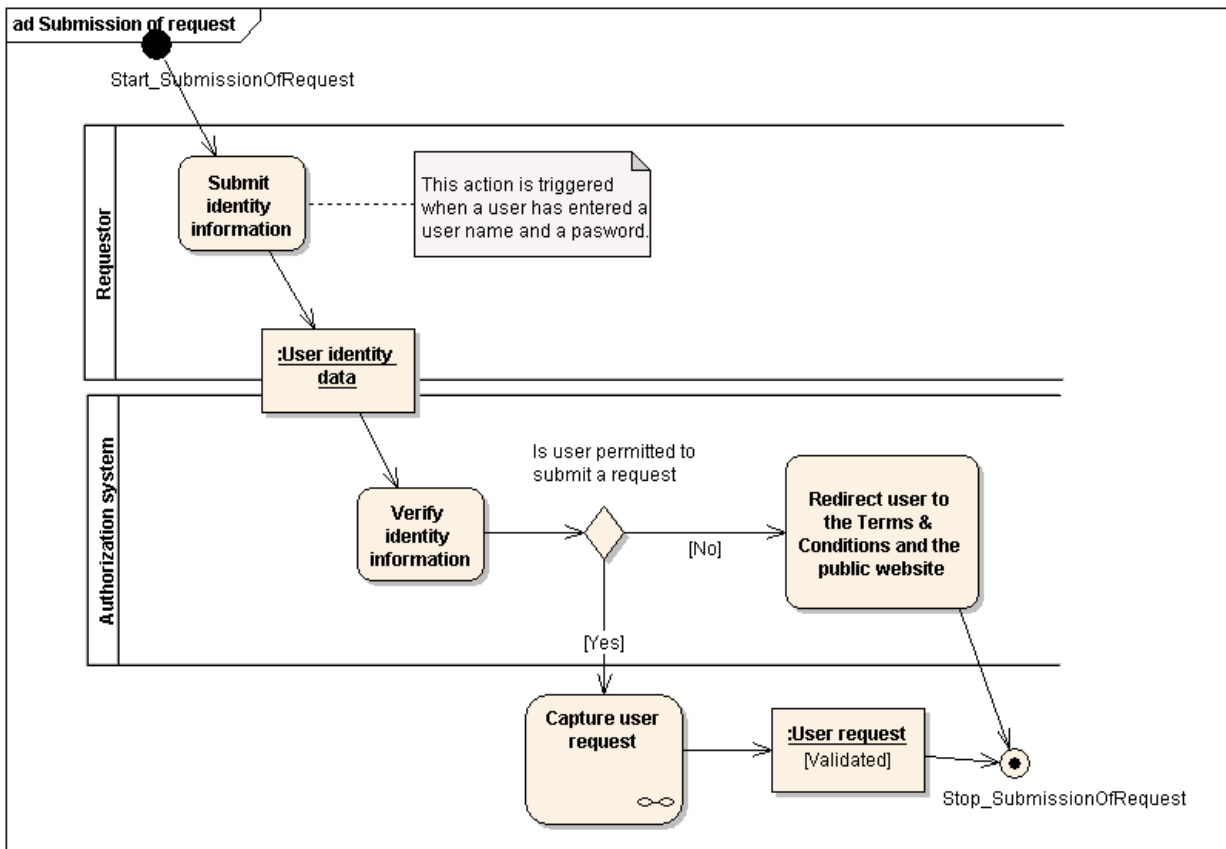


Figure 4 Submission of request

| Used data objects in activity |
|-------------------------------|
| User identity data |
| User request [Validated] |

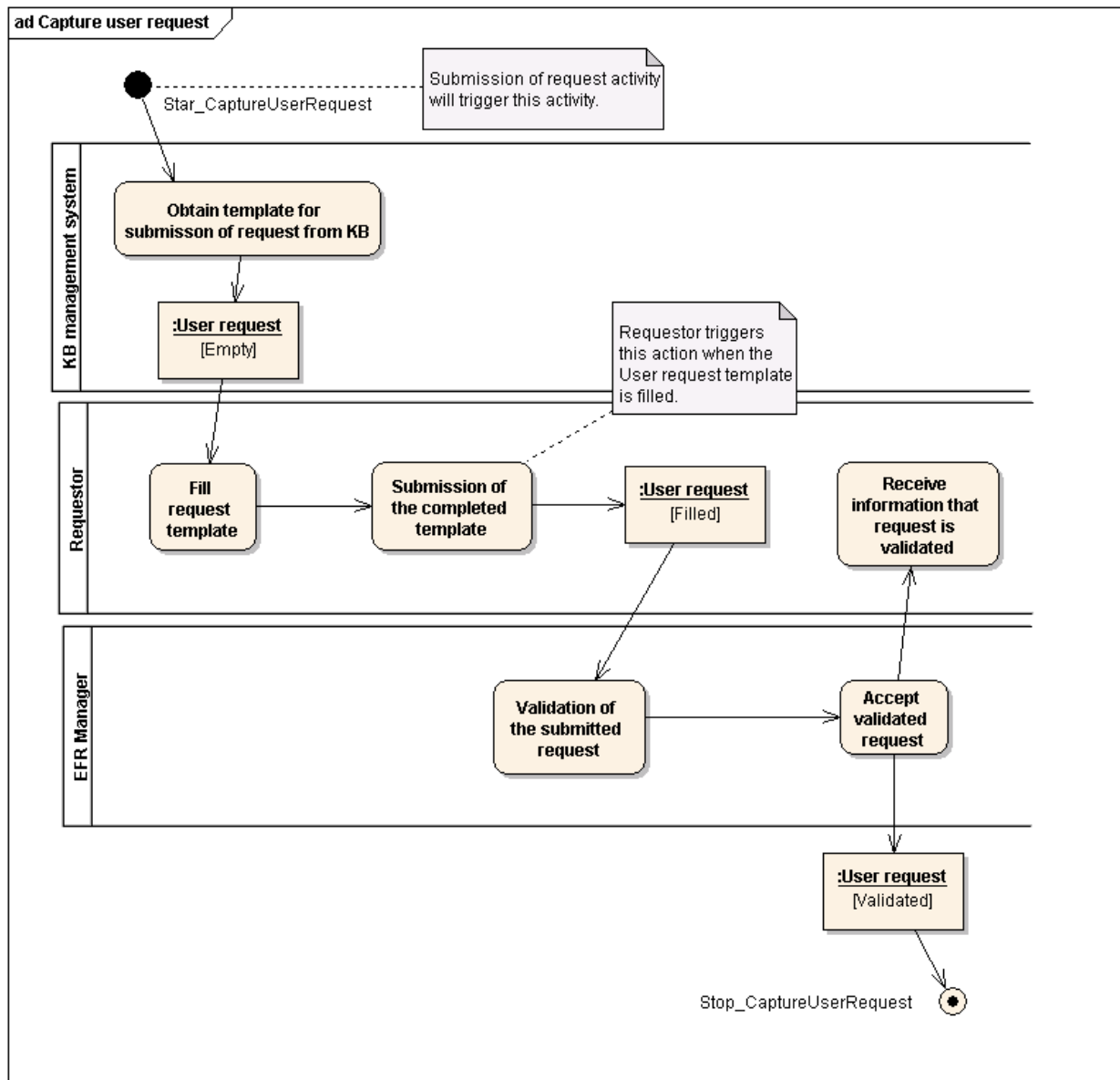


Figure 5 Capture user request

| Used data objects in activity |
|-------------------------------|
| User request [Empty] |
| User request [Filled] |
| User request [Validated] |

Scenario Building and Analysis

Figure 6 represents the *Scenario building and Analysis* at the root level and Figure 7, Figure 8, Figure 9, and Figure 10 refine these activities.

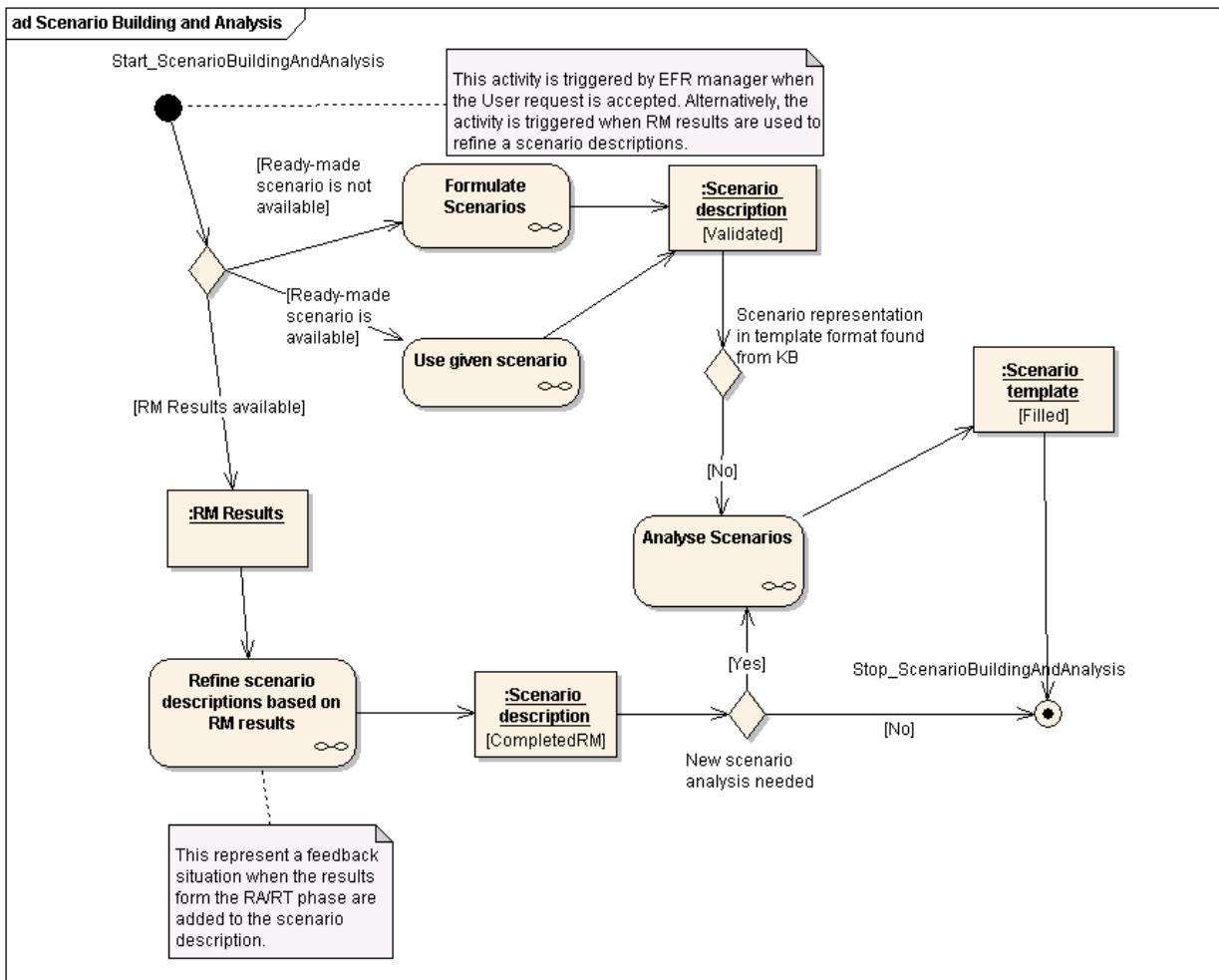


Figure 6 Scenario building and Analysis

| Used data objects in activity |
|------------------------------------|
| Scenario description [Validated] |
| Scenario template [Filled] |
| RM results |
| Scenario description [CompletedRM] |

Figure 7 and Figure 8 represent alternative ways to construct the *Validated description of a set of scenarios* data object.

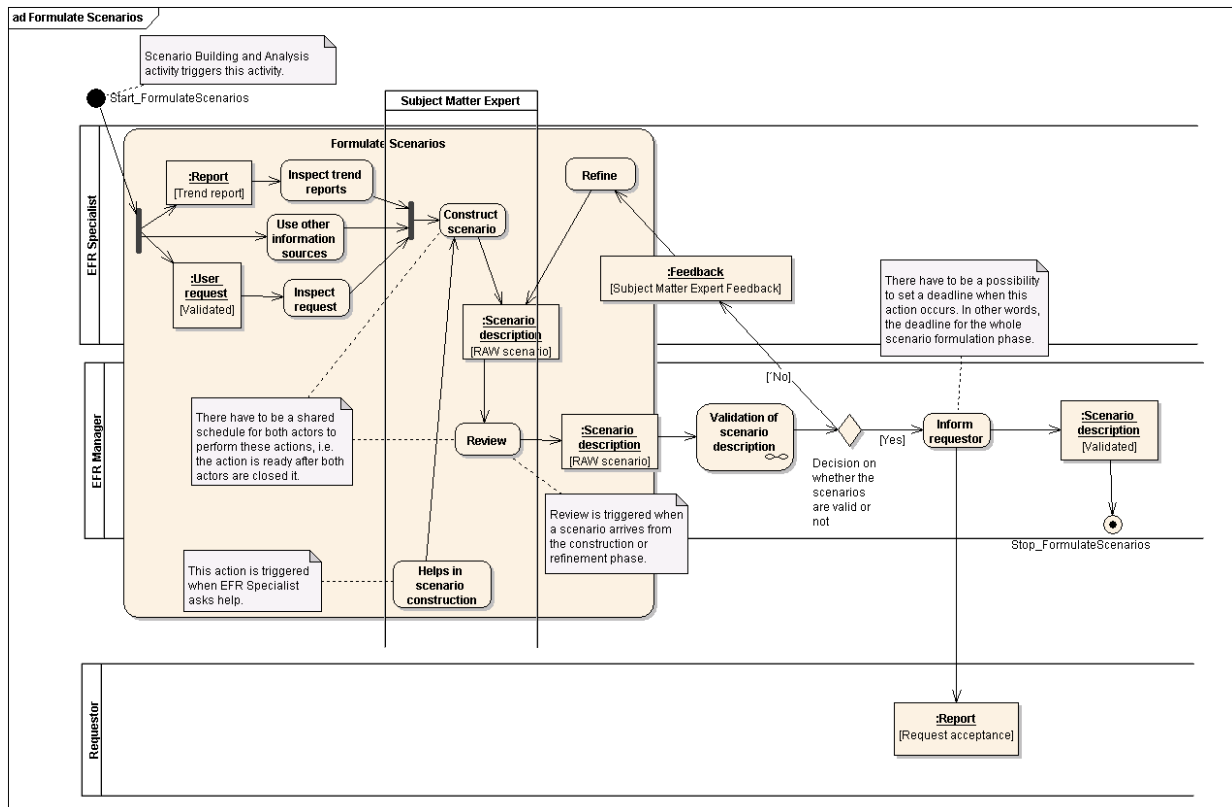


Figure 7 Formulate scenarios

| Used data objects in activity |
|---|
| Report [Trend report] |
| User request [Validated] |
| Scenario description [RAW scenario] |
| Scenario description [Validated] |
| Report [Request acceptance] |
| Feedback [Subject Matter Expert Feedback] |

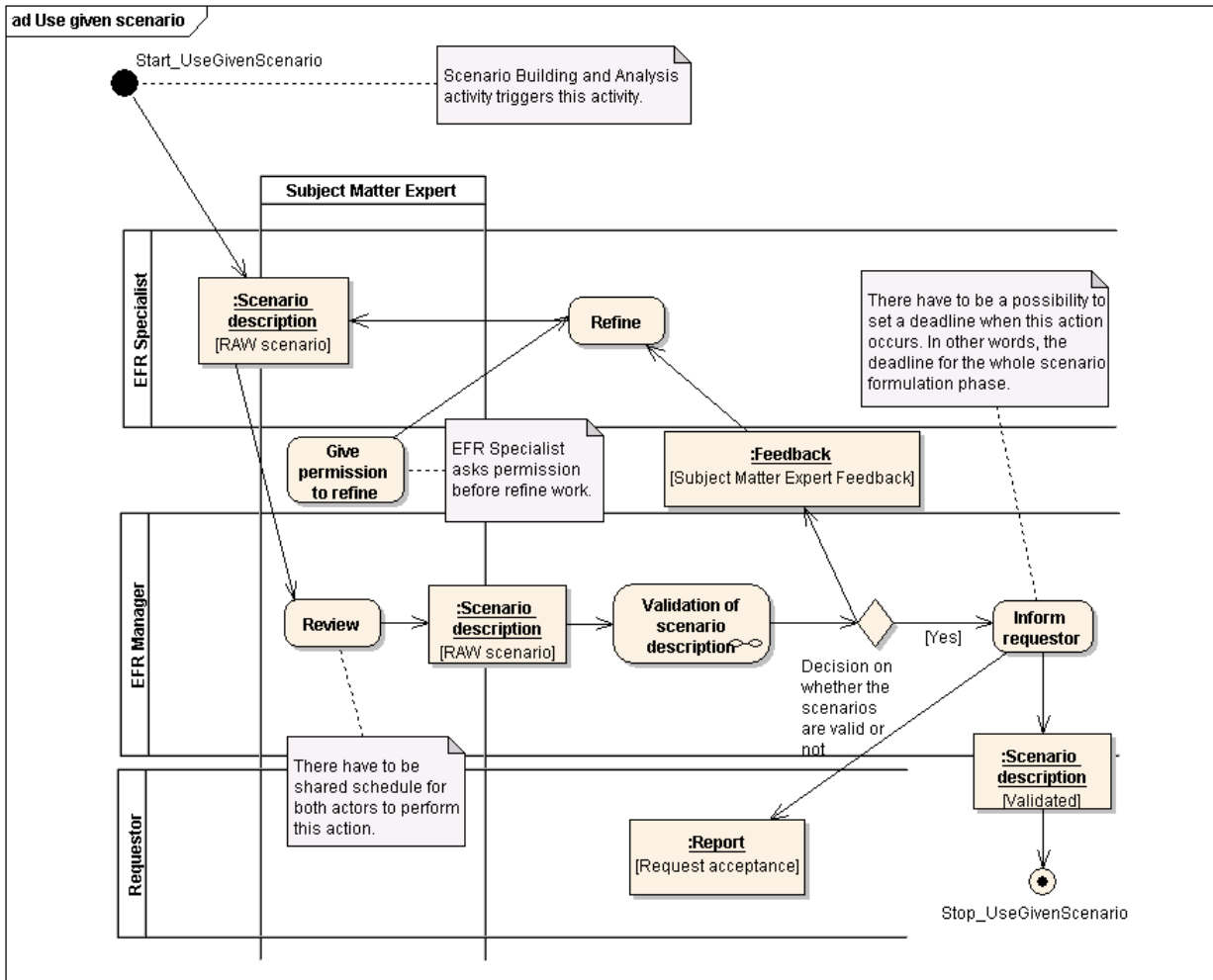


Figure 8 Use given scenario activity

| Used data objects in activity |
|---|
| Scenario description [RAW scenario] |
| Scenario description [Validated] |
| Report [Request acceptance] |
| Feedback [Subject Matter Expert Feedback] |

Figure 9 represents the *Validation of scenario description*.

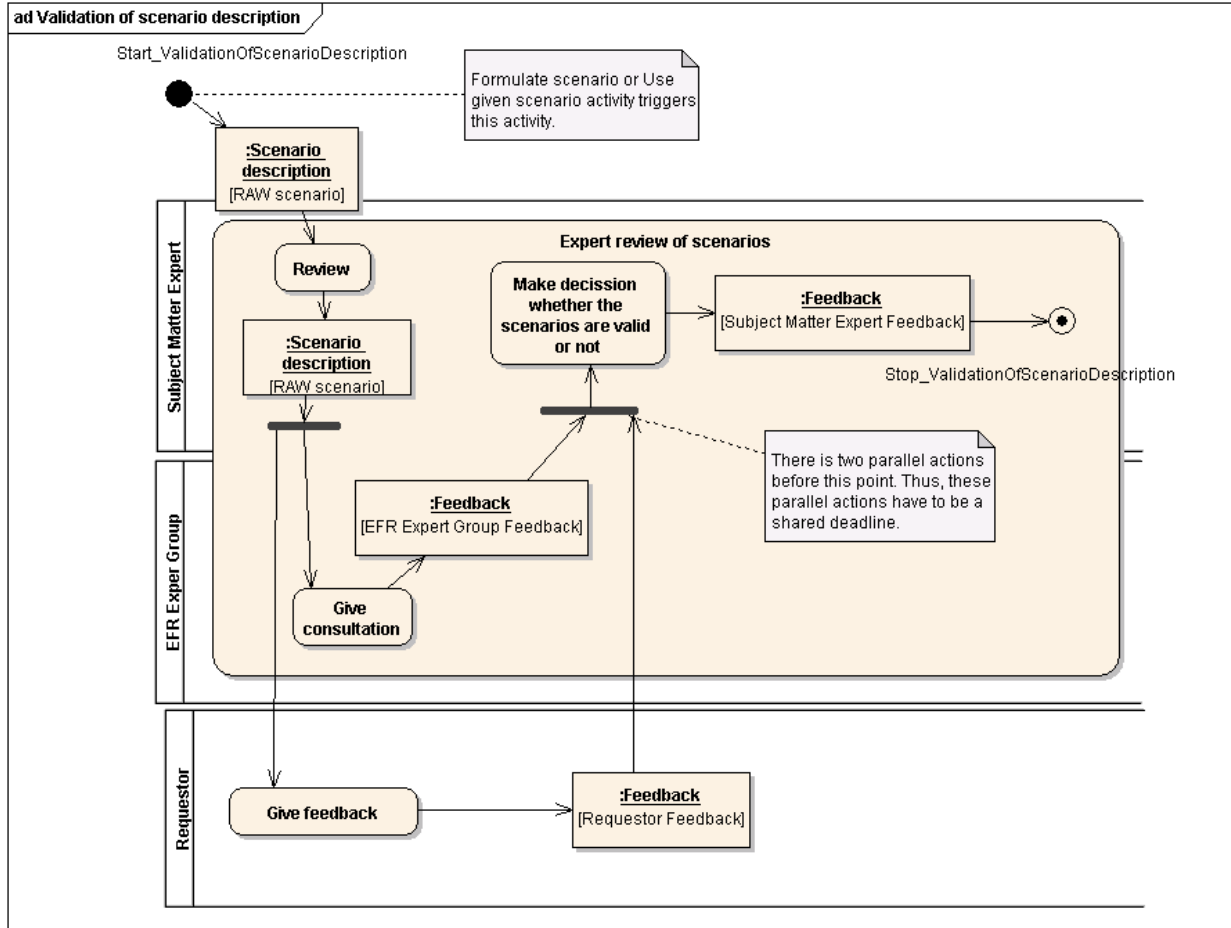


Figure 9 Validation of scenario description

| Used data objects in activity |
|---|
| Scenario description [RAW scenario] |
| Feedback [EFR Expert Group Feedback] |
| Feedback [Requestor Feedback] |
| Feedback [Subject Matter Expert Feedback] |

Figure 10 represents *Analyse scenarios* activity. In this activity, a text based scenario description is formulated into the template form called Scenario template. EFR specialist and subject matter expert formulate scenarios together as a working group.

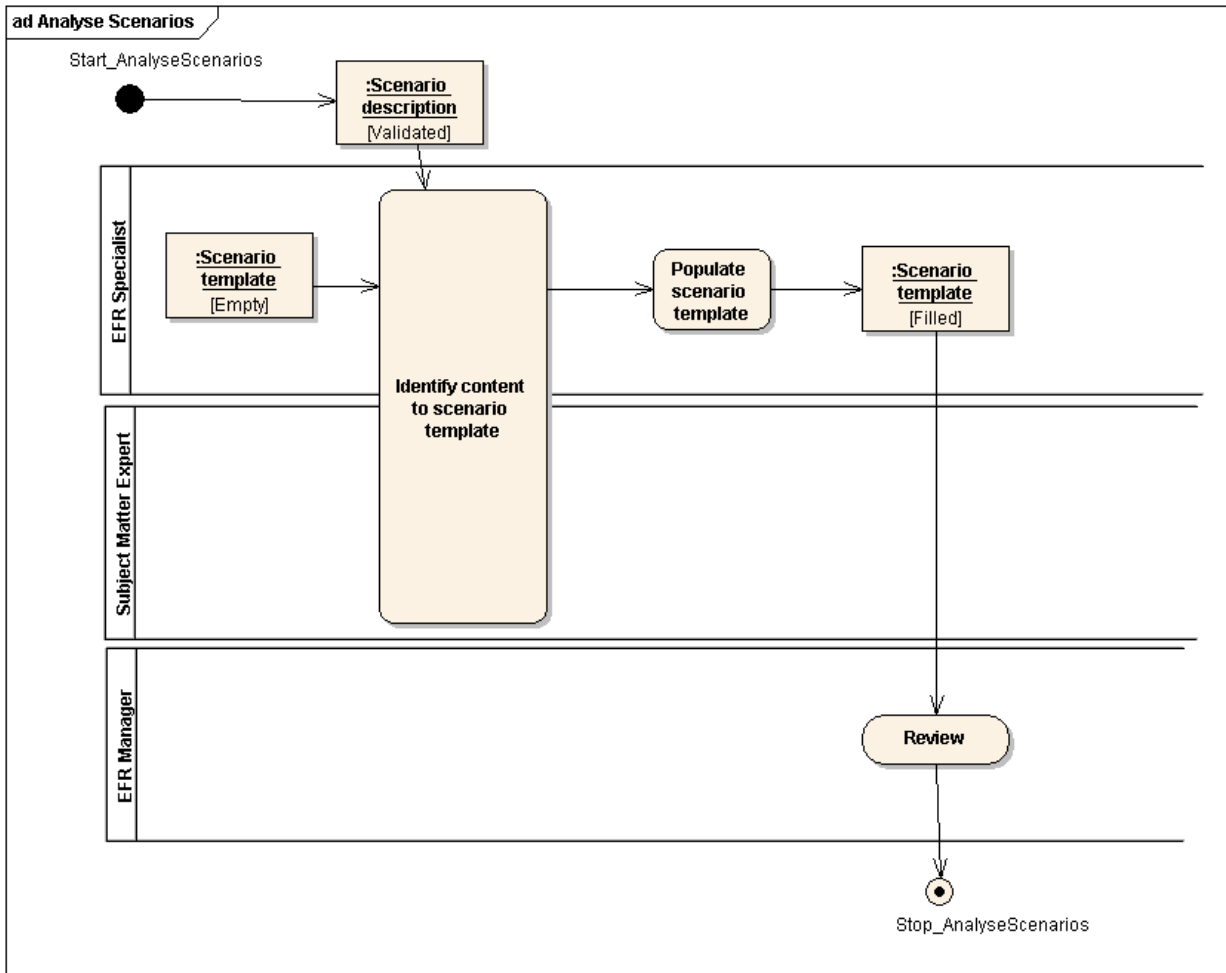


Figure 10 Analyse scenarios

| Used data objects in activity |
|----------------------------------|
| Scenario description [Validated] |
| Scenario template [Empty] |
| Scenario template [Filled] |

Figure 11 shows the case when a feedback loop from the *Risk Management* phase to the scenario building is used.

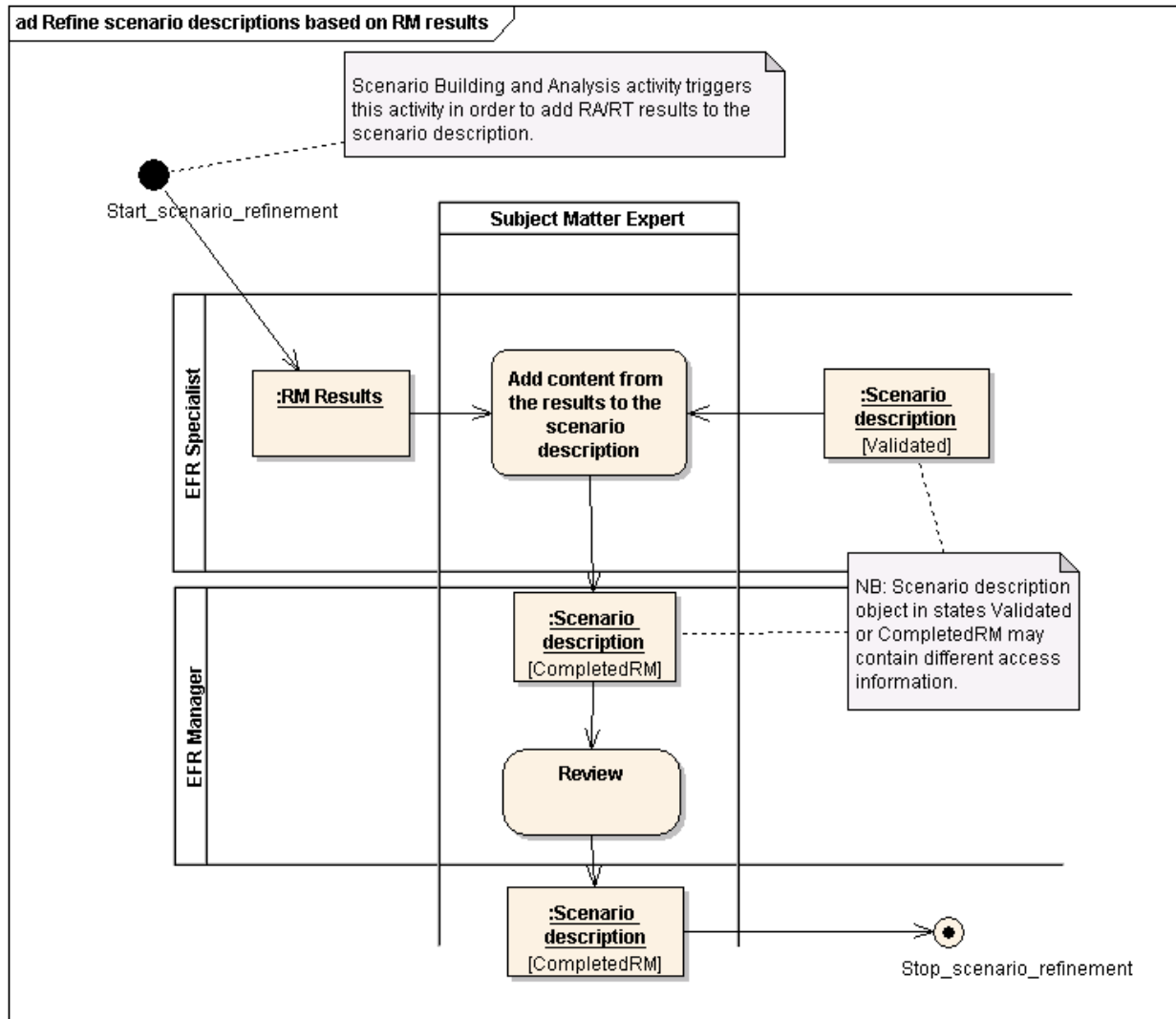


Figure 11 Refine scenario descriptions based on RM results

| Used data objects in activity |
|------------------------------------|
| RM results |
| Scenario description [CompletedRM] |
| Scenario description [Validated] |

Information Dissemination

Figure 12 and Figure 13 describe *Information dissemination*.

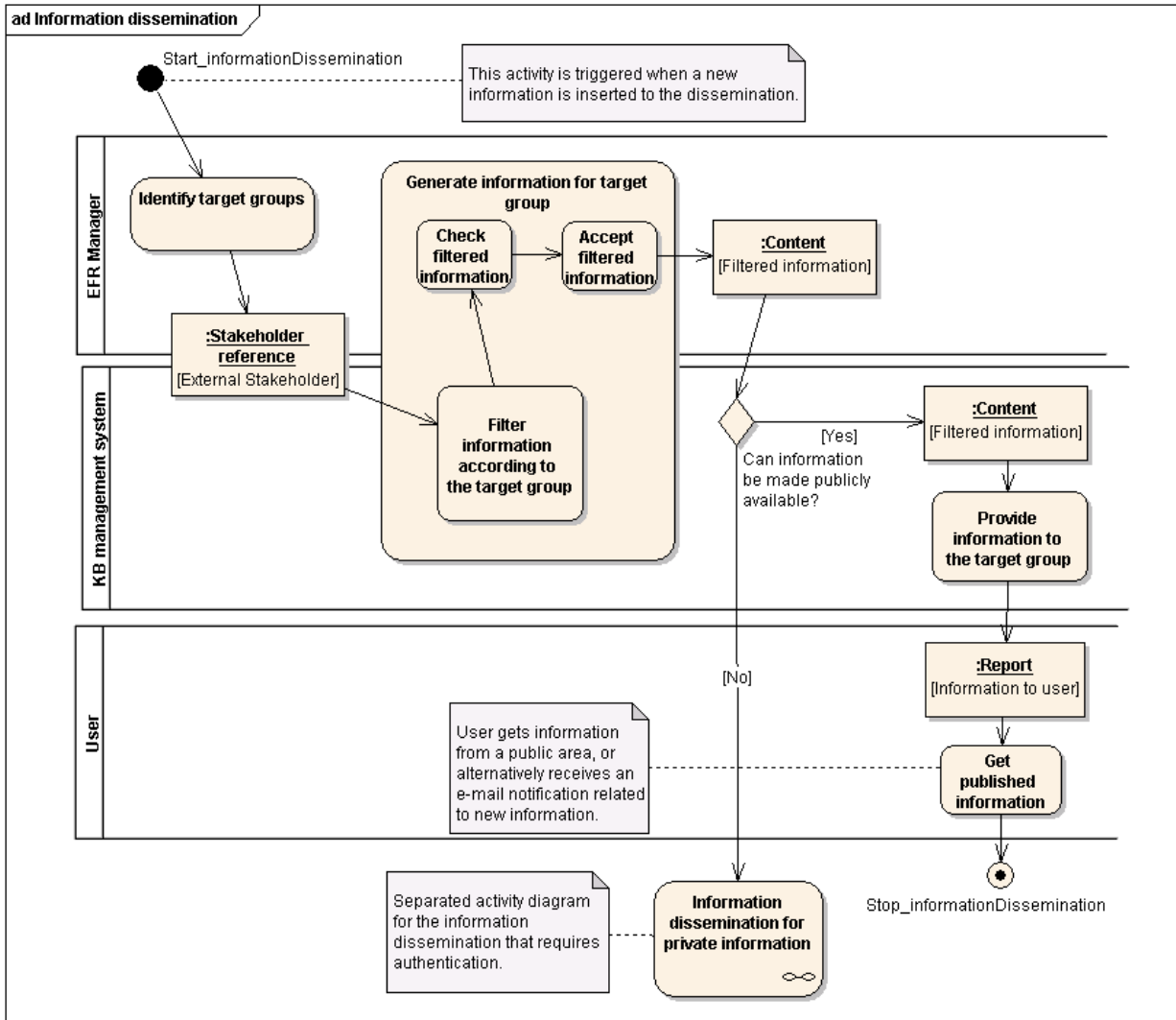


Figure 12 Information dissemination

| Used data objects in activity |
|--|
| Stakeholder reference [External Stakeholder] |
| Content [Filtered Information] |
| Report [Information to user] |

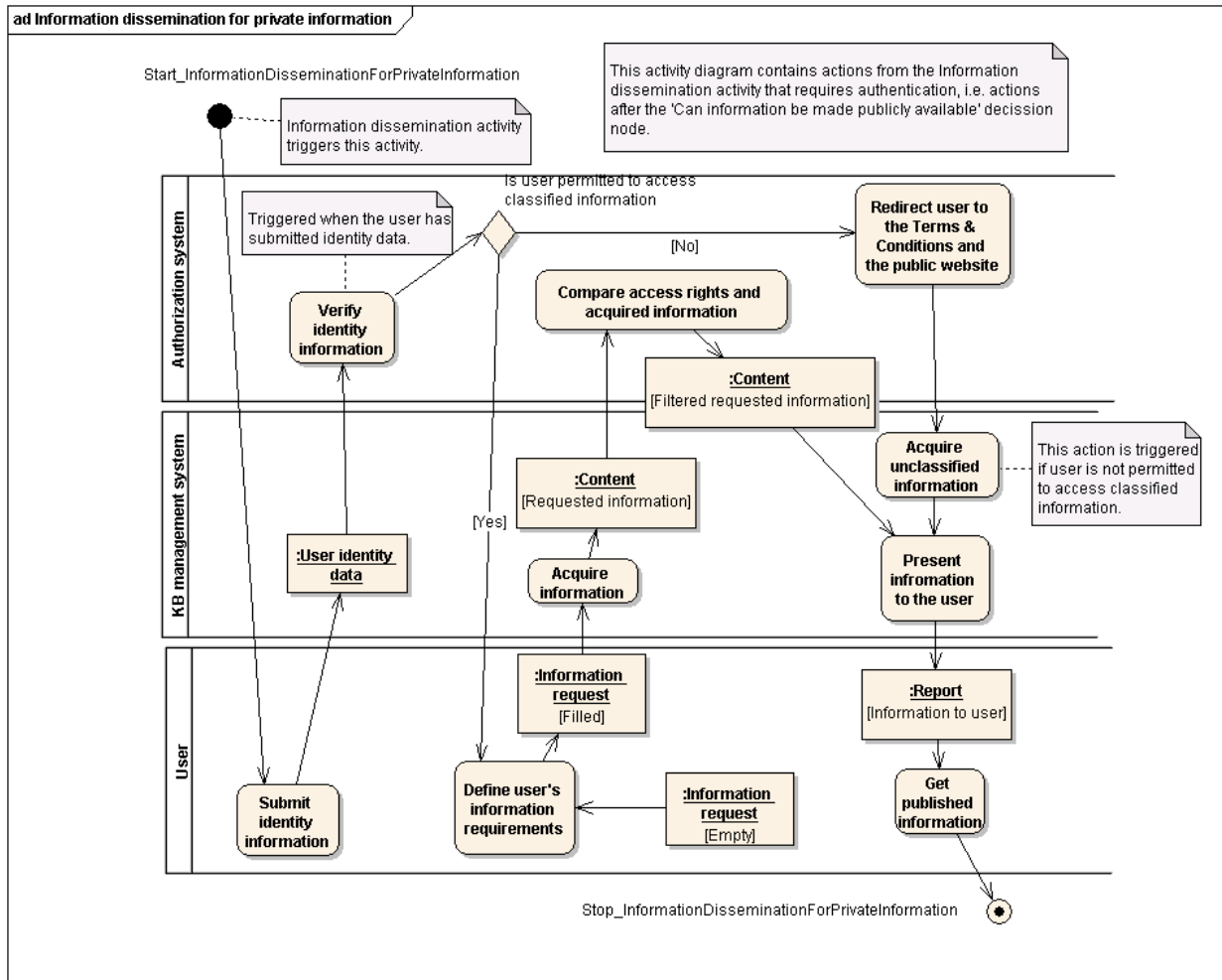


Figure 13 Information dissemination for private information

| Used data objects in activity |
|--|
| Content [Filtered requested information] |
| Information request [Empty] |
| User identify data |
| Information request [Filled] |
| Content [Requested information] |
| Report [Information to user] |

4. Interface to risk management

This section describes interfaces from the *EFR* scenario definition to the *RM/RA method* and forward to the *Information Management*, especially the data flows from the *Scenario Analysis* (SA) activity to the *Risk Assessment* (RA) and the data flows from the *Risk Assessment* (RA) and *Risk Treatment* (RT) to the *Information Dissemination*. *Scenario Analysis* produces detailed scenario data which is exploited in the *Risk assessment* and the *Risk Treatment* activities. The data objects that are collected from the scenario description are presented in Figure 16.

The input/output data of RA and RT activities are presented in Table 1. Needed input data that is produced inside the RA/RT phase can be recognized from the table, e.g. I.2.1 O.1.5 means that the input 2.1 is the output 1.5. The rest of the objects (which are not produced inside the RA/RT phase) are listed and defined in Table 2.

| Action | Input data | Output |
|---------------------------------|--|--|
| Risk Assessment activity | | |
| 1. Identification of risks | I.1.1 Impact statement I.1.2 Historical information I.1.3 Risk id methodology I.1.4 Assessment tools | O.1.1 Disregarded threats just. O.1.2 Likelihood data O.1.3 Identification method doc. O.1.4 Values O.1.5 Relevant vulnerabilities O.1.6 Relevant impacts O.1.7 Relevant threats |
| 2. Analysis of relevant risks | I.2.1 O.1.5 I.2.2 Risk limits I.2.3 Asset class. scheme I.2.4 O.1.1 I.2.5 O.1.3 I.2.6 O.1.7 I.2.7 O.1.2 I.2.8 Existing controls I.2.9 O.1.6 I.2.10 Relevant detailed assets I.2.11 O.1.4 | O.2.1 Impacts relative to assets O.2.2 Threats relative to assets O.2.3 Classified assets O.2.4 Controls relative to assets O.2.5 Risks relative to assets O.2.6 Risks relative to asset groups |

| | | |
|------------------------|---|-------------------------------|
| 3. Evaluation of risks | I.3.1 O.2.4 I.3.2 O.2.1 I.3.3 Assessment activities criteria I.3.4 O.2.2 I.3.5 O.2.6 I.3.6 O.2.3 I.3.7 Asset class. scheme I.3.8 O.2.5 | O.3.1 Risk treatment decision |
|------------------------|---|-------------------------------|

| Risk Treatment activity | | |
|-------------------------------------|--|---|
| 4. Identification of options | I.4.1 Assessment activities criteria I.4.2 O.3.1 I.4.3 Risk limits for criteria I.4.4 Risk treatment options | O.4.1 Class. risk treatment options |
| 5. Development of action plan | I.5.1 Priority scheme I.5.2 Add org. roles I.5.3 Planning methodology I.5.4 O.4.1 | O.5.1 Responsibility assignment O.5.2 Resource assignment O.5.3 Action plan |
| 6. Approval of action plan | I.6.1 Presentation techniques I.6.2 O.5.3 | O.6.1 Approved Activity Lists |
| 7. Implementation of action plan | I.7.1 O.6.1 I.7.2 Add considered activities I.7.3 Implementation cost reporting I.7.4 Cost indicators I.7.5 Reporting scheme | O.7.1 Project progress reports O.7.2 Implement. progress reports O.7.3 Overview of costs O.7.4 Coordinated activity list |
| 8. Identification of residual risks | I.8.1 Internal stakeholder events | O.8.1 Evaluated residual risks |

Table 1 Activities and transmitted data in the RA/RT

Table 2 explains the input data objects for the *Risk Assessment*, which are not coming from a previous action.

| RM/RA input data | Producing Process/Activity | Comments |
|-------------------------|----------------------------|--|
| Identification of risks | | |
| I.1.1 Impact statement | Scenario Analysis Activity | <p>The impact statement must describe the forms of loss or damage to assets using the following criteria:</p> <ul style="list-style-type: none"> • Human • Monetary • Technical • Operational <p>It is also critical to describe the escalation of damage as time passes following the incident.</p> <p>During the scenario analysis activity the subject matter experts, taking into account the perspective of the stakeholders and any historical data as well as trend reports will contribute to this output.</p> |

| RM/RA input data | Producing Process/Activity | Comments |
|-----------------------------------|--------------------------------|--|
| I.1.2 Historical information | Information Collection Process | Historical Information when available provides a starting point in calculating the likelihood of the stated impacts. The information is being compiled in the information collection process where subject matter experts identify relevant sources and extract the required information. Candidate sources include scientific papers, www publications, vendor or consulting firm reports and the opinions of the appointed subject matter experts. |
| I.1.3 Risk id methodology | Select Subject Matter Experts | The selection of the appropriate risk identification methodology is the responsibility of the EFR experts. The requestor/user of the EFR service may supply a preference and reasoning for the application of a specific methodology and this will be factored into the EFR specialists' decision. The methodology has to be selected early in the process to allow for the timely recruitment of the required experts. |
| I.1.4 Assessment tools | Select Subject Matter Experts | A list of assessment tools can be suggested by EFR experts or the recruited Risk Management experts. |
| Analysis of relevant risks | | |
| I.2.2 Risk limits | Scenario Analysis Activity | We will supply this later. |
| I.2.3 Asset class. scheme | Scenario Analysis Activity | The asset classification scheme will be developed during the analysis of the scenario. Asset classification for tangible assets can be achieved by taking into account asset interdependencies, asset's monetary value, and assets role in the operation of the service/application/technology. Asset classification for intangible assets will have to take a more complex approach. Several of the following aspects will have to be factored in, such as the perceived value by the asset owner and the level of liability the system has concerning the asset. Liability may be defined by legislation, regulations, contracts, cultural aspects and social rules. |

| RM/RA input data | Producing Process/Activity | Comments |
|--------------------------------------|----------------------------|---|
| I.2.8 Existing controls | Scenario Analysis Activity | The list of “existing controls” of a future application can be compiled integrating input by the requestor, preliminary architecture or design documents and the knowledge opinion of the subject matter experts. The information collection process will provide the data set that will be used during the scenario analysis to produce the definite list of “existing controls”. |
| I.2.10 Relevant detailed assets | Scenario Analysis Activity | Fully detailed description of the assets has to be achieved by the end of the scenario analysis face. The detail available will be dependent on the data provided by the requestor, information provided by subject matter experts and inquires to vendors, web searches, research prototypes, trends, etc. Relevance will already be assessed using the asset classification scheme. |
| Evaluation of risks | | |
| I.3.3 Assessment activities criteria | Scenario Analysis Activity | By the end of the scenario analysis phase several aspects of the scenario will be better understood and documented by EFR and Subject matter experts. Impacts, their severity, frequency of occurrence and assessed stakeholder sensitivity to these impacts will be amongst the criteria to be used during the assessment activities. |

Table 2 List of data objects that are not coming from the previous actions

There are several *Risk assessment* methods available and each method needs a different input data. In order to facilitate the *Risk Assessment* and *Treatment*, all data produced in the *Scenario Analysis* should be stored as a structured format, e.g. as a scenario template, to the knowledgebase. Therefore, the assessment methods that need different input data can revisit the filled scenario template and collect the needed data objects.

The *Scenario Analysis* has to produce small data chunks in order to make data flowing fluently. Thus, it is important to design a proper template for the scenario data – after that there is no need for several scenario templates. Hence, we suggest that assessment method issues are not taken into account in the *Scenario analysis* phase, and the scenario data is always stored as a template where data is collected in the assessment phase. Figure 16 in Section 6 presents the defined structure for the scenario template.

Interface between the *Risk Management* and the *Information Management* can be implemented in a similar way. The output data can be arranged to a template form and each template or field in the template can get different access rules, which facilitates a data filtering in the *Information Dissemination*. It is worth noting that the requestor can give restrictions related to

the dissemination of the results of RA/RT. The information from the *Risk Management* is named as *RM results* and this data object is used in a feedback loop from the *Risk Management* to the *Scenario building and analysis* phase.

5. Transmitted data elements

This section, i.e. Table 3, describes the transmitted data elements between actions and activities. Name of the data object can be found directly from the activity diagrams in Section 3. In addition, data elements can contain different states or types – these are also described in this table. It is important to notice that in reality each data object is transmitted via the knowledgebase, since even activity diagrams transmit these data objects directly between actions.

| No | Name of data object | Details | |
|----|----------------------|---|--|
| N1 | Scenario template | Structured template for <i>Scenario Description</i> , related data model is represented in Figure 16. EFR specialist and Subject matter expert identify items from the <i>Scenario Description</i> and fill them to the Scenario template. All fields are not necessarily filled (depends on the scenario description). Contains at least following attributes: <ul style="list-style-type: none"> • Asset • Context • Technology / application • Timeframe • Data • Used subject matter expert States: Empty, Filled | |
| | | Empty | A blank scenario template without data. Referred in: Figure 2 |
| | | Filled | <i>Scenario Description</i> as a template form. Referred in: Figure 2, Figure 6 and Figure 10 |
| N2 | Scenario Description | Text based scenario description, i.e. this description does not contain a scenario in the structured format. Describes for example, actors, timeframe, technologies / applications, context, used information, etc. in a prose form. E.g. Word or PDF document. States: RAW scenario, Validated, CompletedRM | |
| | | RAW scenario | This description can come from the requestor or alternatively EFR specialist and the requestor construct it as a co-operation. Referred in: Figure 7, Figure 8 and Figure 9 |
| | | Validated | Reviewed and accepted <i>RAW scenario</i> . Thus, contains same information and in addition acceptance date. Referred in: Figure 6, Figure 7, Figure 8, Figure 10 and Figure 11 |

| | | | |
|----|--------------|--------------------------------|---|
| | | CompletedRM | <i>Scenario Description</i> that contains appropriate results from the <i>RA</i> and <i>RT</i> phases, thus its access rights can differ from the <i>Validated Scenario Description</i> . Referred in: Figure 6 and Figure 11 |
| N3 | Feedback | | Free formatted text that contains comments and refinement suggestions related to the <i>Scenario Description</i> . Contains at least: <ul style="list-style-type: none"> • Identification information of the feedback giver • Data and time • Name of the reviewed document • Feedback Types: Requestor Feedback, Subject Matter Expert Feedback, EFR ExpertGroup Feedback |
| | | Requestor Feedback | Feedback data that is collected from the <i>Requestor</i> . Referred in: Figure 9 |
| | | Subject Matter Expert Feedback | The <i>Subject matter expert</i> produces this data based on the <i>Requestor</i> and <i>EFR Expert Group Feedback</i> . Referred in: Figure 7, Figure 8 and Figure 9 |
| | | EFR Expert Group Feedback | Feedback and consultation from the <i>EFR expert group</i> . Referred in: Figure 9 |
| N4 | User request | | Template for capturing Requestor's scenario request in the structured format. NB: <i>User</i> in this phase is called <i>Requestor</i> Template has to contain at least: <ul style="list-style-type: none"> • 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 Following information is not mandatory, but helps the RM phase if available. <ul style="list-style-type: none"> • Impact statement, i.e. the importance for assets • Asset classification scheme • Suggestion for the used Risk id methodology • Existing controls States: Empty, Filled, Validated |
| | | Empty | Empty template Referred in: Figure 5 |

| | | | |
|----|---------------------|--|---|
| | | Filled | Template filled by the <i>Requestor</i> Referred in: Figure 5 |
| | | Validated | Validated and accepted template. Referred in: Figure 2, Figure 4, Figure 5 and Figure 7 |
| N5 | User Identity data | Contains attributes: <ul style="list-style-type: none"> • User name • Organization • Sector • Role in the organization • Role in the workflow • Access rights Referred in: Figure 4 and Figure 13 | |
| N6 | Information request | User defines his/her information needs in this template. Based on this data element search for the knowledgebase is executed. Query input contains at least: <ul style="list-style-type: none"> • Technology (for example there can be a drop-down menu for technologies in the template) • Application • Key words States: Empty, Filled | |
| | | Empty | Empty <i>Information request</i> template Referred in: Figure 13 |
| | | Filled | Filled <i>Information request</i> template Referred in: Figure 13 |
| N7 | Report | Types: Trend Report, Requestor Deliverable, Information to user, Request Acceptance. | |
| | | Trend Report | E.g. Word / PDF documents or web sites. Referred in: Figure 2 and Figure 7 |
| | | Information to user | Information set that is delivered to the user. This data varies relating to user's access rights and User's information requirements. Referred in: Figure 2, Figure 12 and Figure 13 |
| | | Request Acceptance | Reply message to the <i>Requestor</i> that her/his request is accepted and related <i>Scenario Description</i> is ready for analyse. <ul style="list-style-type: none"> • Request's name • Acceptance date Referred in: Figure 7 and Figure 8 |

| | | | |
|-----|-----------------------|--|---|
| N8 | Content | Content from the knowledgebase and its different states during the information dissemination. States: Filtered Information, Requested Information, Filtered Requested Information | |
| | | Filtered Information | Information that can be made available to the target group. This means that information is arranged based on access rights {public, internal, confidential}. NB: all information from the knowledgebase can be disseminated if the user has sufficient rights. Referred in: Figure 12 |
| | | Requested Information | This data is queried from the knowledgebase based on the <i>Information request</i> object. Therefore, this information can contain any available information from the knowledgebase (NB: access rights are checked later on) Referred in: Figure 13 |
| | | Filtered Requested Information | This is the data object that is received when the <i>Requested Information</i> object is filtered according to access rights. Thus, from this data the <i>Information management system</i> produces the Report called <i>Information to user</i> . Referred in: Figure 13 |
| N9 | Stakeholder Reference | Stakeholders: Subject Matter Experts, External Stakeholder | |
| | | Subject Matter Experts | Selected subject matter experts. List of expert names and their organizations. Referred in: Figure 2 |
| | | External Stakeholder | List of user names, organizations etc. Also access rights {public, internal, confidential} are taken into account in this data element. Referred in: Figure 12 |
| N10 | RM results | Results of the risk assessment and treatment phases. This data object can be disseminated if the requestor has given permission in the <i>Submission of request</i> activity. In addition, this data object is used to refine <i>Scenario Description</i> when the feedback loop from the <i>RM</i> phase to the <i>Scenario building</i> is exploited. Referred in: Figure 2, Figure 6 and Figure 11 | |

Table 3 Used input / output data elements

6. Data model

Figure 14 contains data objects and their relationships in the EFR process. Data elements' names comply with the names used in Table 3. Instead, the data model in Figure 16 represents data elements from a *Scenario template* viewpoint, i.e. these elements are included in the *Scenario template*.

Each disseminated data object has to have an access information {public, internal, confidential} element. However, from the clarity reasons these elements are not included in Figure 14, but every document has to have this information.

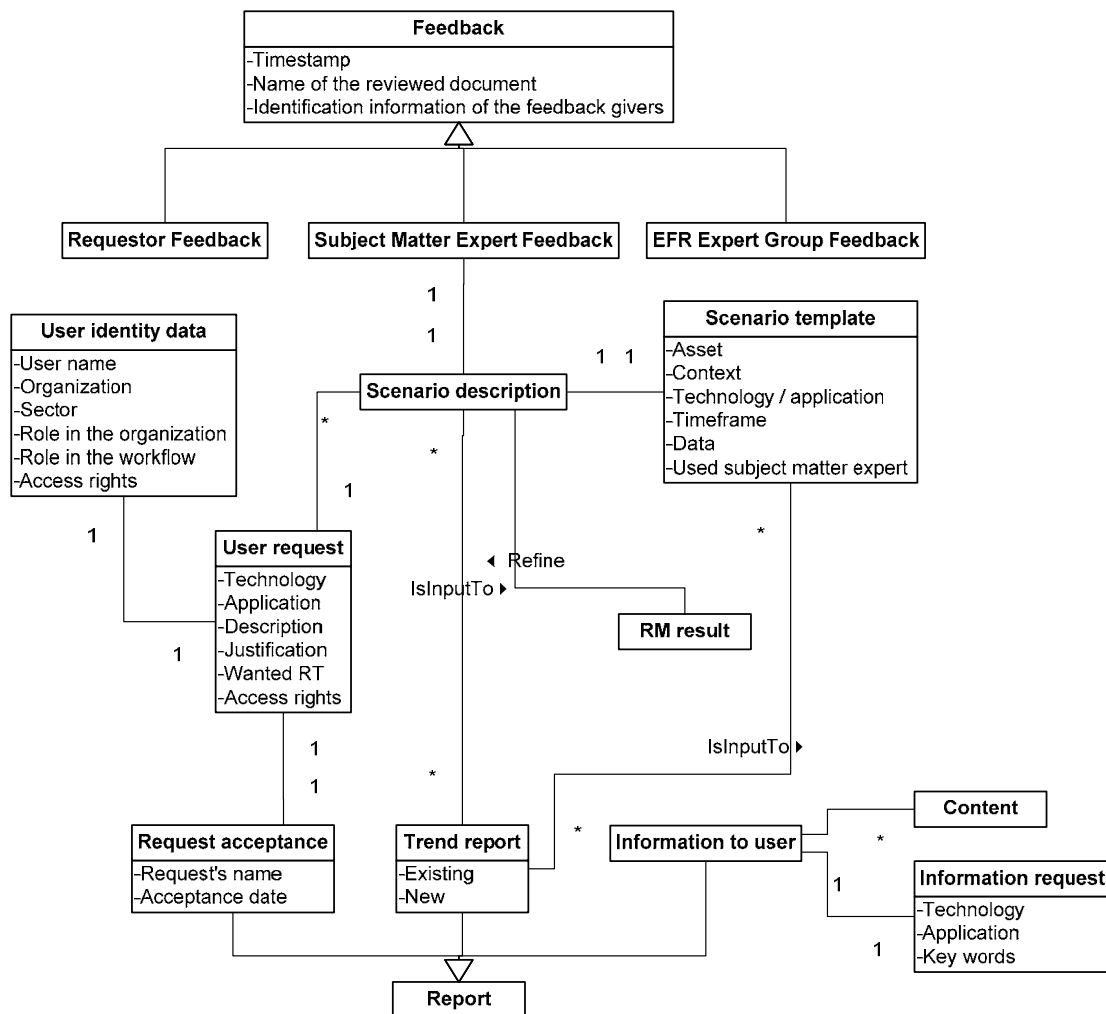


Figure 14 Data model of the EFR process.

Figure 15 present the boundary between the *Scenario building* and *Risk assessment* phases. Thus, threats and vulnerabilities are not included in the *Scenario building* phase in this project. Instead, *Scenario building* names assets, i.e. Application / device, Technology and Data / information.

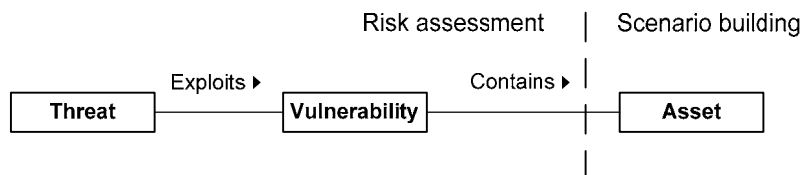


Figure 15 Boundary between Scenario building and Risk assessment

Figure 16 represents data elements that are collected to the *Scenario template* from the *Scenario description*. When the *Scenario template* is filled it receives access information {public, internal, confidential}. This information restricts the dissemination of the whole scenario.

The *Scenario template* is filled in the *Scenario analysis* activity based on *Scenario description*. However, *Impact statement*, *Risk limits*, *Asset classification scheme*, *Existing controls*, *Relevant detailed assets*, and *Assessment activities criteria* which will be needed in the RM phase are also decided in this phase. These fields are not presented in Figure 16 because it depicts entities residing in the *Scenario description*.

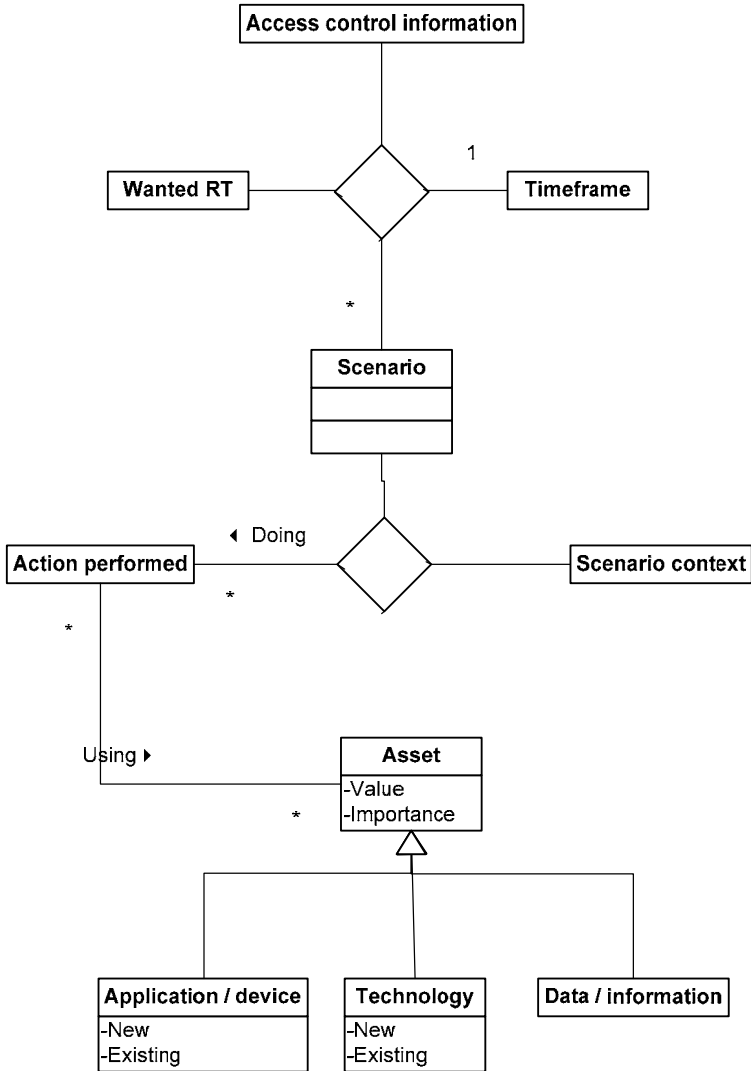


Figure 16 Scenario template data model

7. Conclusions

This document describes EFR workflow by means of UML activity diagrams. These activity diagrams specify actors for each action in the workflow and transmitted data objects between actions. Interface from the *Scenario building and analysis* phase to the *Risk management* phase is also defined. Furthermore, data models for describing the primary relationships between data objects are also described. As such, the document can be used as a specification for the prototyping and subsequent implementation projects.

Design document

If you would like to **include a Back Cover** at the end of your document:

- “insert” “picture: from file” browse to the file **Publications_Back_cover.jpg** This contains a background as well as the Agency’s contact details.
- Right-click on it and go to “format picture”. Edit size at **100%**, text wrap at “**behind text**”.
- Click **advanced**, go to **picture position: horizontal** alignment should be **left** relative to **page** and **vertical** alignment should be **top** relative to **page**. De-activate the “**move with text option**”

If you do not use the back cover, insert the address on the front page under the brand bar