HOPEX Enterprise Risk Management

User Guide

HOPEX V2

INTRODUCTION TO HOPEX ENTERPRISE RISK MANAGEMENT

HOPEX Enterprise Risk Management offers a simple and flexible solution for managing organization operational risks to optimize sustainable company performance.

The tool integrates different risk management approaches to ensure compliance with Basel II and Solvency II regulations and to the COBIT framework.

It helps risk managers set up a consistent risk management methodology adaptable to their specific company requirements.

HOPEX Enterprise Risk Management supports all aspects of risk management - risk environment definition, risk identification and analysis, risk assessment and treatment.

- ✓ "Risk Management Process", page 6
- ✓ "HOPEX Enterprise Risk Management Profiles", page 8

RISK MANAGEMENT PROCESS

Associated with all HOPEX Suite products, **HOPEX Enterprise Risk Management** enables identification, assessment and remediation of risks.

Identifying, analyzing and contextualizing risks

The aim of risk analysis is to obtain a good understanding of risks. Risk analysis must take risk sources into account as well as positive or negative risk consequences.

The analysis phase associates a risk with:

- risk types
- risk factors (or causes)
- consequences
- objectives

Contextualization of a risk enables risk classification by:

- on the one hand their type
- on the other the objects to which they relate

The same risk can relate to several component types:

- an entity
- a process
- a business line
- a site.

Assessing Risks

After having identified and analyzed the risks faced by the enterprise, the next step is to estimate their importance so as to highlight the most important risks to be remediated.

It is particularly important to identify risk causes so that the risks themselves will be treated and not just their symptoms.

Risks are assessed taking into account:

- their occurrence frequency
- their impact

This assessment will serve as the basis for determining how the risks will be managed.

Standard reports are supplied to simplify risk assessment. For more details, see "HOPEX Enterprise Risk Management Reports", page 55.

Two possibilities are proposed:

- Direct assessment, which allows an expert to specify global assessment of a risk on a given date,
- Assessment by campaign, which enables precise assessment of your risks by entity from standard questionnaires.

Remediating Risks

Remediating risks involves:

- identification of the various options possible
- assessment of these options
- preparation and implementation of remediation plans.

The design of risk remediation measures should be based on a perfect understanding of the risks concerned; this understanding is obtained from an appropriate level of risk analysis.

It is not generally profitable, or indeed desirable, to implement all possible risk remediations. It is however necessary to select and implement a combination of the most appropriate of these.

Risk assessment is therefore an essential step in obtaining a list of risks requiring remediation, indicating their priority.

CONNECTING TO HOPEX ENTERPRISE RISK MANAGEMENT

The menus and commands available in **HOPEX Enterprise Risk Management** depend on the profile with which you are connected.

Connecting to the HOPEX Enterprise Risk Management Solution

To connect to **HOPEX Enterprise Risk Management**, see HOPEX Common Features, "HOPEX Desktop", "Accessing HOPEX (Web Front-End)".

HOPEX Enterprise Risk Management Profiles

In **HOPEX Enterprise Risk Management**, there are default user profiles with which specific rights and accesses are associated. The profiles available are:

- Risk Functional Administrator
- Risk Manager and Local Risk Manager
- Business User (ERM)

Risk Functional Administrator

The functional administrator has rights on all objects and workflows.

He/she prepares the work environment and creates elements required for management of risks.

Manages:

- environment description
  - entities and processes
  - regulatory environment
  - IT resources

☛ *For more details on description of the environment, see the "Defining the Environment for Solutions", page 463 chapter.*

- users and assignment of roles.

Can intervene in:

- declared risks
- assessment campaigns
- action plans and actions

Risk Manager

To adapt to centralized or decentralized risk management, **HOPEX Enterprise Risk Management** distinguishes:

- the ***Risk Manager***
- the ***Local Risk Manager***

The Risk Manager is responsible for execution of the following tasks on risks within his/her responsibility domain:

- Risk identification
- Direct assessment
- Assessment campaign management
- Action plan definition
- Analysis and follow-up report creation

Business User

The business user has a simplified desktop accessing questionnaire functions, action plans and objects for which he/she is responsible:

- Risks and controls
- Questionnaires
- Action plans

HOPEX Enterprise Risk Management Desktop Presentation

The menus and commands available in **HOPEX Enterprise Risk Management** depend on the profile with which you are connected.

Functional Administrator space

The functional administrator has several desktops:

- **Administration** desktop.
- **Environment** desktop, which enables definition of the work environment.
- **ERM** desktop, which presents tabs corresponding to the main risk management steps:
  - **Home**: enables easy access to the different folders and objects for which the user is responsible
  - **Risk Library**: enables access to the list of risks and controls. Direct assessments can be made from this tab
  - **Campaign Management**: enables management of risk assessment by campaigns.
  - **Remediation**: enables specification and implementation of action plans and controls designed to treat risks.
  - **Reports**: accesses reports enabling analysis and follow-up of implementation of controls and risks.
  - **Document Library**: enables access to documents linked to risk management.

☛ *For more details, see "Risk Functional Administrator", page 8.*

Risk Manager space

The Risk Manager has two desktops **Environment** and **ERM** identical to the desktops of the Risk Functional Administrator.

☛ *For more details, see "Risk Manager", page 9.*

Business User space

The business user has only the **Home** tab, presenting the objects for which he/she is responsible.

☛ *For more details, see "Business User", page 9.*

MANAGING RISKS

To control risks, it is necessary to identify and qualify the risks encountered in the execution of a process.

> 🕮 *A risk is a hazard of greater or lesser probability to which an organization is exposed.*

When risks have been analyzed and assessed, management determines how each of these risks should be treated. **HOPEX Enterprise Risk Management** offers tools that simplify creation and analysis of risks to identify the most important of these and set up adapted corrective or preventive actions.

The following points are covered here:

✓ "Accessing Your Tasks", page 12
✓ "Describing Risks", page 13
✓ "Organizing Risks", page 16

> ☛ *For more information on use of analysis reports proposed on risks, see "HOPEX Enterprise Risk Management Reports", page 55.*

Accessing Your Tasks

To access the different folders and objects for which you are responsible:

1. Select **Risk > Home > My Desktop**.

Your desktop allows you to access:

- Your **Responsibilities**
  - assessment questionnaires
  - risks
  - Controls
  - Action Plans
  - Campaigns
  - Reports
- Your **Scope**
  - risks
  - Controls
  - Action Plans
- Your **Notifications**
  - Unread notifications
  - Read notifications

DESCRIBING RISKS

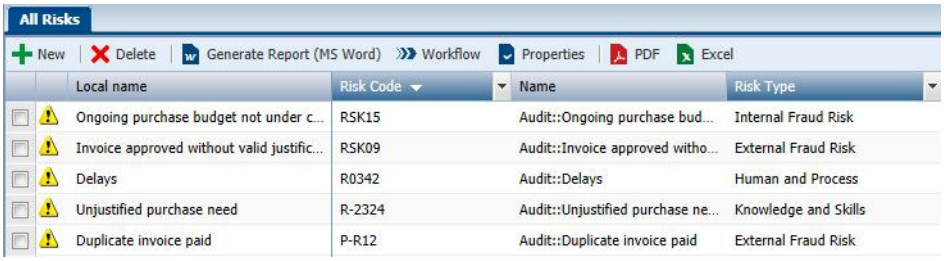
Accessing the Risk List

To access the list of risks:

- Select **Risk** > **Risk Library > Risks**.

From the **Risks** folder you can access different lists of risks:

- All Risks
- Key Risks, which are highest level risks
- Risks Without Control.



Risk Properties

Risk properties are described in paragraph "Risks and Controls", page 471.

☛ *To be able to assess risks in the framework of assessment campaigns by questionnaires, you must first specify certain properties. For more details, see "Preparing the Work Environment", page 31.*

MANAGING RISKS

The risk creation process is managed by a workflow. Therefore only certain profiles are authorized to create, submit, validate or reject a risk.

☛ *For more details on the risk creation workflow and associated notification messages, see "Risk Workflow", page 76.*

Creating risks

To create a risk:

1. Select **Risk** > **Risk Library > Risks > Risks > All Risks**.
   You obtain the list of all risks.
2. Click the **New** button.
3. Press key <F2> to modify the **Name** of the risk.
4. Open the properties page of the risk.
5. Specify the risk **Owner** responsible for entering information on the risk before submitting it for validation.

Duplicating Risks

Duplicating a risk enables copying of all properties of an existing risk.

To duplicate a risk:

1. In the **Risk Library**, select **Contextualization > List View**.
2. Click the risk that you want to duplicate and select **Duplicate**.
   A new risk carrying the same name as the initial risk appears in the list of risks.

The duplicated risk is identical to the original risk: all characteristics and links to repository objects are identical. The action plans are duplicated. Only risk assessments are not duplicated.

Validating a Risk

The steps in the validation process of a new risk are the following:

- Having specified the characteristics of a new risk, the risk creator (who is also the risk owner) can :
  - **Submit** the risk.
  The risk manager receives a notification by mail and the new risk appears with status "Submitted".
- When a risk has been submitted, the Risk Manager can:
  - **Validate** the risk, which takes status "Validated".
  A notification is sent by mail to the user defined as "Owner".
  - **Reject** the risk.
  In this case, the risk takes status "Rejected", but is not deleted.

ORGANIZING RISKS

Contextualization of risks enables their classification according to their type on the one hand, and the objects to which they relate on the other. The same risk can relate to several component types:

- **Entities**,
- **Processes**, **Business Processes** and **Organizational Processes**,
- **Objectives**.

HOPEX Enterprise Risk Management enables you to easily connect risks with the objects to which they relate.

Reports presenting risk contextualization are available as standard. For more details, see "Location Matrix", page 56.

Accessing Risks from their Context

To obtain the lists of risks according to their context:

1. Select **Risk** > **Risk Library > Risk Trees**.
   You obtain the list of risk classification folders.
2. You must expand the tree to obtain the list of risks attached to an object.

Contextualizing Risks

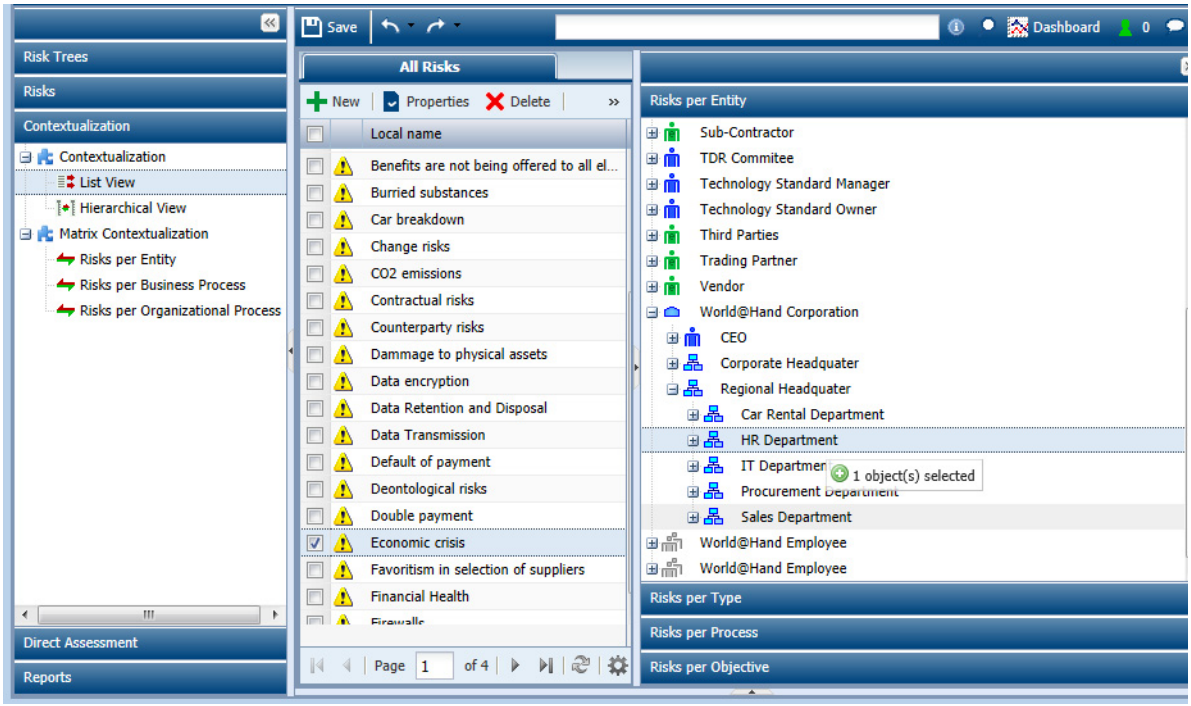
HOPEX Enterprise Risk Management enables you to connect easily the risks and objects to which they relate: an entity, a process.

To contextualize risks, three possibilities are proposed:

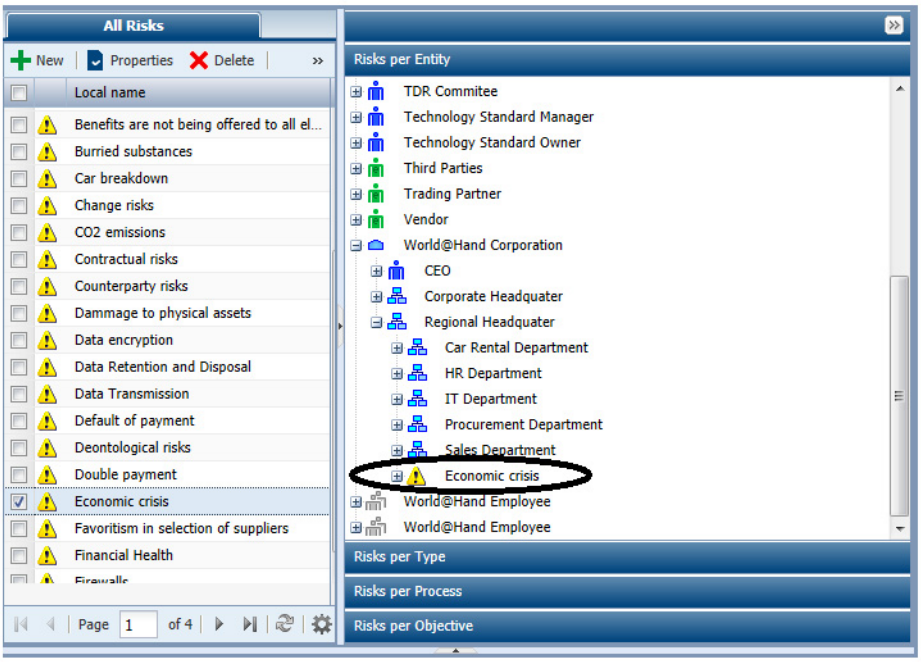
Using lists to contextualize risks

To connect a list of risks to an object:

1. Select **Risk** > **Risk Library > Contextualization > Contextualization > List View**
   In the edit area, you will find:
   - on the left, this list of risks
   - on the right, the contextualization trees
2. Expand the folder of the object type that interests you, for example **Risks by Entity** and select the entity that interests you.
3. In the left of the edit area, select the risks that interest you.
4. Holding the right-hand mouse button down, drag the selected risks under the entity to which you want to connect them.



The list of selected risks appears on the right, under the selected entity.



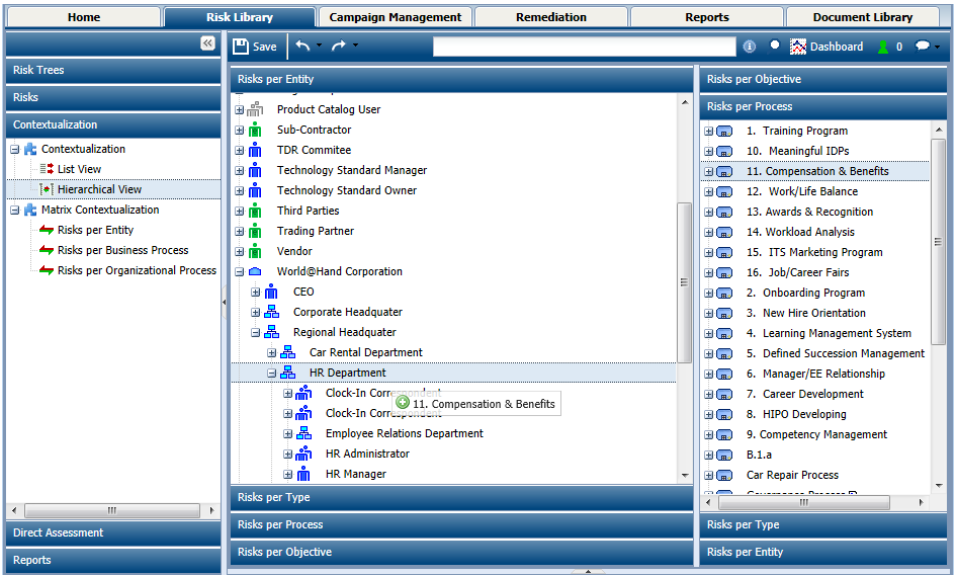
Using trees to contextualize risks

Contextualization trees allow you to ensure consistency between risks connected to objects of different types.

If for example you want to connect risks relating to an organizational process to the entity responsible for implementation of this process:

1. Select **Risk** > **Risk Library > Contextualization > Contextualization > Hierarchical View**
   Two contextualization trees appear right and left of the edit area.
2. In the contextualization tree on the right, select for example **Risks by Processes** and expand the tree to display the risks connected to the process that interests you.
3. In the contextualization tree on the left, select for example **Risks by Entity** and expand the tree to display the entity that interests you.

4. Select the risk that interests you and holding the mouse button down, drag the selected risk under the entity to which you want to connect it.



Using a matrix to contextualize risks

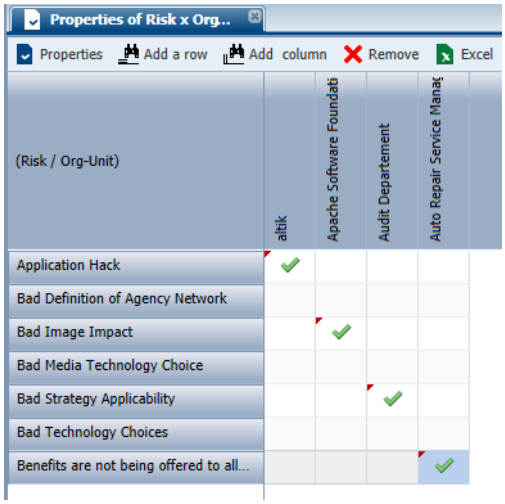
You can use a matrix to connect risks to entities or processes.

To connect risks to entities:

1. Select **Risk** > **Risk Library > Contextualization > Matrix Contextualization > Risks by Entity**.
2. At the top of the edit area, click command **Add Line**.
3. In the dialog box that opens, click  .
4. Select the risks that interest you and click **OK**.
   The selected risks are displayed as rows in the edit area.
5. Proceeding in the same way, select the entities by clicking **Add Column**.
   The selected entities appear as columns in the edit area.

6. If you click in the empty cell at the intersection of risk and entity, you connect the risk to the entity.
   The symbol ✔ appears in the cell.

   ☛ *In a similar way you can disconnect a risk from an entity.*



To disconnect a control from an entity:

❱ In the matrix, click again in the cell concerned.
The green tick disappears. The link between risk and entity is deleted.

ASSESSMENTS WITH HOPEX ENTERPRISE RISK MANAGEMENT

After having identified and analyzed the risks encountered by the enterprise, it is essential to highlight the most important of these in order to remediate them.

In **HOPEX Enterprise Risk Management**, risk assessment is qualitative: the impact of a risk is described by terms corresponding to a predefined scale (for example 1 to 4). In this way mapping of risks can be established to quickly identify the most critical risks.

HOPEX Enterprise Risk Management proposes two assessment possibilities:

- Direct assessment, which allows an expert to specify global assessment of a risk on a given date,
- Assessment by campaign, which enables precise assessment of your risks by entity from standard questionnaires.

> ☛ *This chapter explains how to start assessments. To configurer these, see the **HOPEX Assessment guide, "Assessment Templates" chapter".***

✓ "Risk Assessment Types", page 22
✓ "Assessing risks directly", page 23
✓ "Assessing Risks by Questionnaires", page 26
✓ "Assessment Campaign Workflow Steps", page 31

Risk Assessment Types

A risk measurement is designed to give values, in a specific context, for the different characteristics such as risk likelihood or impact.

Characteristics values can be specified:

- from the risk properties page, for more details see "Using Direct Assessment", page 23
- from a risk assessment matrix, for more details see "Using the Direct Assessment Matrix", page 25
- or via an assessment form, for more details, see "Assessing Risks by Questionnaires", page 26

Results of risk assessment can be displayed in dedicated reports whick make it easier to analyse the assessed risks. For more details, see "HOPEX Enterprise Risk Management Reports", page 55.

ASSESSING RISKS DIRECTLY

Direct assessment provides, at a given date, assessment of a risk on an entity of the organization.

You can carry out:

- direct assessment from a risk
- multiple assessment from a table

Using Direct Assessment

You can create new assessments to globally assess a risk on all objects of the organization to which it is connected (ie. entities).

This is an "expert view" assessment.

Creating direct assessments

To create an assessment:

1. Select a risk and open its properties.
2. Select the **Assessment** tab.
3. Click the **Evaluate** button.
4. Select the context in which the risk is to be assessed, then click **Next**.

   ☛ *The contexts are available only if there is more than one.*
5. Specify characteristics values:
   - **Impact**: the impact of the risk when it occurs.
   - **Likelihood**: the probability that the risk will occur.
   - **Control level**

     🕮 *Control level characterizes efficiency level of control elements deployed (controls) to assess the risk.*
6. Specify the assessment date.
7. Click **OK**.

   An assessment is created.

   The following values are calculated:
   - gross risk

     🕮 *The inherent (or gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence likelihood or impact of this risk. This is the result of multiplying impact value and likelihood value before taking account of risk prevention or reduction measures.*
   - net risk

     🕮 *The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk. is the difference between the Inherent Risk and the Control Level.*

Consulting assessment answers

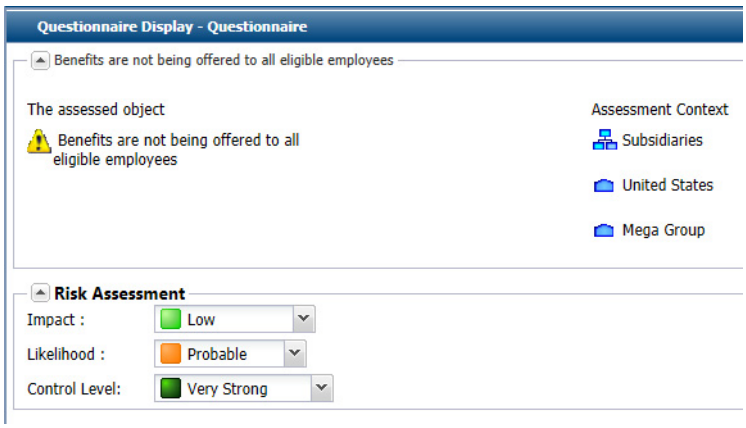
The manager can view answers entered by the respondent when performing direct assessment. He/she can also decide to modify values calculated from these answers if he/she considers them inappropriate.

To view answers used to calculate assessed characteristics values:

- In the **Assessment** tab of the assessed object properties, right-click the measurement that interests you and select **Display Node**.

  ☛ *This menu is not available in the context of multiple assessment.*

  Answers used as the basis for calculation of values appear. They are in read-only only.



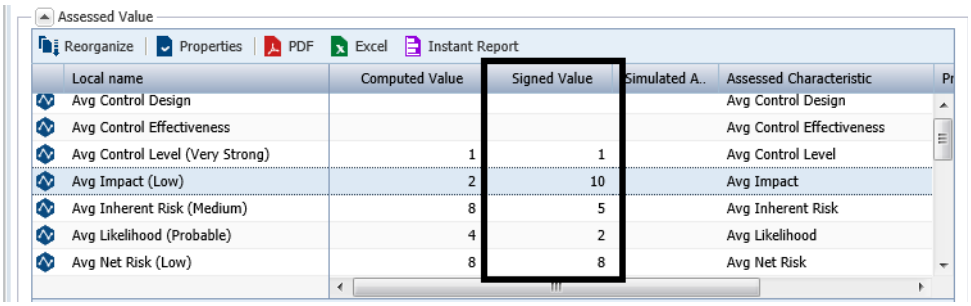
The responsible/manager can decide to modify values resulting from answers.

To modify assessed characteristics values:

1. Open the properties of the assessment you want to modify.

2. Modify values in the **Signed Value** column for each assessed characteristic value.
   These values replace values calculated from answers given by the respondent.

   ☛ *Initial values are visible in the **Calculated Value** column.*



☛ *The values specified in the **Signed Value** column are not used in reports supplied by default. You can however call a **MEGA** professional to include these values in your questionnaires.*

Using the Direct Assessment Matrix

You can specify values directly in a matrix to assess several risks simultaneously.

To assess several risks simultaneously:

1. In the **Risk** desktop, select **Risk Library > Direct Assessment > Multiple Assessment Table**.
   An empty table is displayed in the edit area.
2. Click **Connect Objects to be Assessed**.
   A tree appears.
3. Select the risks that interest you in the context of the relevant entities, and click **OK**.

   ☛ *If assessments have already been carried out, the most recent assessment values are presented in columns.*
4. Click in the cell corresponding to a characteristic for a given risk, for example "Impact".
5. Select the required value.
6. When specification is completed, click **Validate Assessment**.
7. Modify the assessment **Effective Date** if necessary and click **OK**.
   A new assessment is created.

Assessment characteristics are as follows:

- **Impact**: characterizes impact of the risk when it occurs.
- **Likelihood**: characterizes probability that the risk will occur.
- **Control Level**: this characteristic gives an overall assessment of risk control level.

ASSESSING RISKS BY QUESTIONNAIRES

HOPEX Enterprise Risk Management enables assessment of your risks using standard questionnaires. In this way you can improve effectiveness of your internal control systems and minimize your risks.

Assessment questionnaires are sent by electronic mail to the appropriate addressees using customizable deployment modes.

Accessing Assessment Functions

Depending on user profile, you can access assessment functions via different menus.

Profile	Action	Menu
Functional Administrator	- Assign roles to persons of the enterprise - Define the organization (entities, processes,...) - Determine respondents (risk assessors for each entity)	Environment Administration
Risk Manager	- Create assessment campaigns - Create assessment sessions - Follow up assessment sessions	Risk > Manage campaigns
Risk Assessor	- Accept or refuse questionnaires Reply to questionnaires	Risk > Home > My Desktop > My Responsibilities > My Assessment Questionnaires

HOPEX Enterprise Risk Management Assessment Template

Before creating an assessment session, you must first create an assessment campaign and define its scope.

The scope of an assessment session is defined by specifying:

- The list of objects to be assessed and characteristics to be assessed on each of the objects.
- The assessment context: which entities, etc.
- The assessment period.

This scope is defined generically at the level of an assessment campaign by an assessment template.

An assessment template is used as a model for creating campaigns and assessment sessions. The assessment template defines the

assessment scope, the questionnaire template to be used, and if required, the aggregation schemas to be applied for interpretation of global results.

All sessions of the same campaign therefore relate to a globally identical scope.

☛ *It remains possible for the session manager to remove or add elements to the scope specific to a session.*

Accessing assessment templates

An assessment template is proposed as standard with **HOPEX Enterprise Risk Management**. Its objective is to obtain an assessment of risks related to an entity.

To access the assessment template:

1. Select **Risk > Campaign Management > Campaign Management > Preparation > Questionnaire Templates**.
   The "Risk Assessment" assessment template appears.

   ☛ *This template is the same as that used in the framework of direct assessment.*

   ☛ *For more details on the use of this assessment template, see "Assessment template detail", page 28.*

The proposed assessment template uses:

- assessed characteristics
- a questionnaire template

Assessed characteristics

🕮 *An assessed characteristic defines what the assessment seeks to assess. It can be associated with a MetaClass, and more specifically with one of its MetaAttributes, for example: Risk MetaClass, MetaAttribute: Likelihood*

To access the list of assessed characteristics proposed as standard by **HOPEX Enterprise Risk Management**:

1. In the **Risk** desktop, click **Campaign Management > Campaign Management > Preparation > Assessed Characteristics**.
   The list of characteristics appears in the edit area.

These characteristics relate to risk attribute values.

☛ *For each of these attributes, the characteristic assessed can relate to the gross value, maximum value or the average.*

- **Impact**: characterizes impact of the risk when it occurs.
- **Likelihood**: characterizes probability that the risk will occur.
- **Inherent Risk**: gives an assessment of risk consequences.

  🕮 *The inherent (or gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence likelihood or impact of this risk. This is the result of multiplying impact value and likelihood value before taking account of risk prevention or reduction measures.*
- **Control Level**: this characteristic gives an overall assessment of risk control level.
- **Net Risk**: is the difference between the ***Inherent Risk*** and the ***Control Level***.

Questionnaire template

A questionnaire template represents definition of questionnaire content: question group, questions, unique or multiple answers and possible answers. It can be associated with a questionnaire presentation specifying display options. Questionnaires sent to assessors are generated from the definition supplied in the questionnaire template.

To access the questionnaire template proposed as standard by **HOPEX Enterprise Risk Management**:

- In the **Risk** desktop, click **Campaign Management > Campaign Management > Preparation > Questionnaire Templates**.

This questionnaire template relates to assessment of risks from the following characteristics:

- **Impact**: characterizes impact of the risk when it occurs.
- **Likelihood**: characterizes probability that the risk will occur.
- **Control Level**: characterizes efficiency level of control elements deployed (controls) to reduce the risk

Assessment template detail

An assessment template is used as a model for creating campaigns and assessment sessions. The assessment template defines the assessment scope, the questionnaire template to be used, and if required, the aggregation schemas to be applied for interpretation of global results.

The "Risk Assessment" assessment template supplied with **HOPEX Enterprise Risk Management** produces a risk assessment related to an entity.

Assessed characteristics

An assessed characteristic defines what the assessment seeks to assess. It can be associated with a MetaClass, and more specifically with one of its MetaAttributes, for example: Risk MetaClass, MetaAttribute: Likelihood

Assessed characteristics are as follows:

- Impact
- Likelihood
- Inherent risk

  The inherent (or gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence likelihood or impact of this risk. This is the result of multiplying impact value and likelihood value before taking account of risk prevention or reduction measures.

- Control level

  Control level characterizes efficiency level of control elements deployed (controls) to assess the risk.

- Net risk

  The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk. is the difference between the Inherent Risk and the Control Level.

Assessed objects

The objects assessed are risks.

The list of risks to be assessed comprises all risks connected to the entity (assessment object) and to its sub-entities

Respondents

Respondents are persons defined as ***Risk Assessor*** for the entity.

Questionnaire

> 🕮 *A questionnaire proposes a list of predefined questions that can be applied to an event type, control, document, etc.*

The questionnaire relates to characteristics to be assessed for all risks determined as objects of assessment:

- Impact
- Likelihood
- Control level

> 🕮 *Control level characterizes efficiency level of control elements deployed (controls) to assess the risk.*

Aggregation schema

Each specified assessment value is carried by an "assessment node" which describes specified value for a characteristic of a given object (risk, entity or process) in a specific context defined by an entity, a respondent, a process.

"Assessment nodes" can be represented in tree form from a root node, which can be:

- A risk
- An entity
- A process
- A risk type
- An objective

Each node carries all values defined in the assessed characteristics. Results of the aggregation of these values produce aggregation reports.

1. Aggregation - Risk Level per Process

	ERM Avg Impact	ERM Avg Inherent Risk	ERM Avg Likelihood	ERM Impact	ERM Inherent Risk	ERM Likelihood
Operations	Very Low	Low	Probable			
R&D						
Counterparty risks				High	High	Probable
Natural catastrophy						
Fraud & Corruption				Very Low	Low	Probable
Security leaks				Very Low	Low	Possible
Work accidents				Very Low	Very Low	Rare

An aggregation schema is a series of steps enabling consolidation of assessment results according to specified assessment rules.

Aggregation schemas of the **HOPEX Enterprise Risk Management** assessment template define the calculation mode:

- Gross values for each risk.
  In the aggregation report example, values presented are: impact, lilelihood, control level, inherent risk and net risk.
- Calculated values (maximum and average) on entities, processes and risk types.
  In the aggregation report example, values presented are: average values calculated on all risks of a process for impact, likelihood and net risk.

Values associated with a risk 'Ri' are calculated from values given to this risk on each of the entities 'Ej' to which it relates. Assessment nodes taken into account are linked to pairs (Ri, Ej)

- Impact of Ri = Max and Average {Impact of (Ri, Ej) for all j}
- Likelihood of Ri = Max and Average {Likelihood of (Ri, Ej) for all j}
- Inherent risk of Ri = Max and Average {Inherent risk of (Ri, Ej) for all j}
- Control level of Ri = Max and Average {Control level of (Ri, Ej) for all j}
- Net risk of Ri = Max and Average {Net risk of (Ri, Ej) for all j}

ASSESSMENT CAMPAIGN WORKFLOW STEPS

HOPEX enables assessments using standard questionnaires.

The assessment questionnaires are sent to appropriate respondents.

Assessment Principle

Assessment is a mechanism enabling sending of questionnaires to an identified population to obtain assessments (qualitative or quantitative) on identified objects. The assessment is then supplemented by results analysis tools.

Assessment session

An assessment session is an assessment carried out over a determined time period. When an assessment session is published, a questionnaire is sent to targeted users.

Questionnaire

Assessment questionnaires are sent to appropriate respondents.

A questionnaire proposes a list of predefined questions that can be applied to a control.

Assessment campaign

With **HOPEX Enterprise Risk Management**, an assessment session is started in the context of an assessment campaign.

A campaign enables grouping of several sessions.

Assessment Steps

Preparing the Work Environment

Before starting an assessment campaign, you must first prepare the work environment. Check that you have:

- connected risks to at least one entity
- specified a respondent in the **Risk Assessor** field of the entity properties.

Starting a campaign and assessment sessions

For an example of the different steps in starting an assessment campaign, see "Steps of assessment workflow with campaign", page 44.

☛ *To discover all the possibilities offered by **HOPEX**, see "Workflows Linked to Assessments", page 142.*

✓ "Creating Assessment Campaigns", page 32
✓ "Creating Assessment Sessions", page 33
✓ "Deploying Assessment Campaigns", page 35

☛ *The deployment of an assessment campaign is not mandatory. If you are not deploying the assessment campaign, go directly to "Validating Assessment Campaigns", page 36.*

✓ "Scoping Assessment Campaigns", page 35
✓ "Planning Assessment Campaigns", page 36
✓ "Validating Assessment Campaigns", page 36
✓ "Deploying Assessment Sessions", page 36
✓ "Scoping Assessment Sessions", page 37
✓ "Validating Assessment Sessions", page 37
✓ "Starting assessment sessions", page 38

When assessment sessions have been started, you can proceed with:

✓ "Completing Questionnaires", page 39
✓ "Following Up Session and Questionnaire Progress", page 40
✓ "Closing the assessment session", page 42

Creating Assessment Campaigns

🕮 *A campaign enables grouping of several sessions.*

You can create an assessment campaign:

- ***From a template***
  Creating a campaign from a template allows:
  - use of the same template in all assessment sessions.
  - definition and planning of sessions by distributing elements to be assessed between different sessions.
- ***without a template***
  In the case of creation of a campaign without using a template, a template can be specified at the time of creation of each session.

☛ *This section presents assessment campaign creation using the assessment template supplied as standard. Possibilities offered by assessment campaigns without using a template are described in the **HOPEX Assessment** guide.*

To create an assessment campaign:

1. In the **Risk** desktop, select **Campaign Management > Campaign Management > Execution > Campaigns**.
   The list of campaigns appears in the edit area.
2. Click **New**.
   The campaign creation page appears.

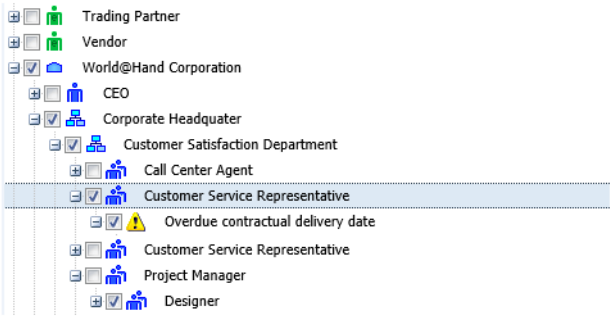
3. Select the "***Risk Assessment***" **Assessment Template**.
4. Modify the **Calendar** if required.

   ☛ *The calendar serves to initialize begin and end dates of the assessment campaign.*
5. Specify the **Begin Date** and the **End Date**.
6. Click **Next**.
7. In the **Scope Selection** page, select an entity.

   ☛ *The tree automatically expands if the **Automatic Expand** box is selected.*

   The tree allows you to select risks assessed ***in their context***.

   A risk is assessed in the context of elements of the branch from the control up to the root.



In the above example, if you select the "Customer Service Representative" entity, all risks and context objects located at a lower level are selected, as well as all parent context objects up to the tree root.

   ☛ *If you deselect a node of a branch, only the child elements of this branch are deselected.*
8. Click **Next**.
9. In the preview window, click **Refresh the Report**.
   Elements that will be assessed appear.

   In particular, you can view:
   - assessed characteristics (defined in the assessment template)
   - assessed objects (risks)
   - context objects (entities)
   - assessment nodes which correspond to risks placed in their context objects, associated with respondents.
   - respondents
10. Click **OK**.

Creating Assessment Sessions

📖 *An assessment session is an assessment carried out over a determined time period. When an assessment session is published, a questionnaire is sent to targeted users.*

Creating Assessment Sessions

To create an assessment session:

1. Open the properties of the campaign and select the **Sessions** tab.
2. In the **Assessment Sessions** section, click **New**.
   You may choose to launch the assessment session later, without specifying when.
3. To do this, in the session launch window, select "**not now**"

   ☛ *This option enables you to complete the assessment session with data, for example with the session owner and the assessment dates. In the framework of an assessment campaign with template, the session template is specified by default. It cannot be modified. For more details on creation of assessment sessions without template (ad-hoc or advanced mode), see "Creating Ad-Hoc Assessment Sessions", page 25 or "Creating Expert Assessment Sessions", page 27.*

   ☛ *You may choose to launch the assessment session now or to schedule it. See "Creating and launching assessment sessions", page 34.*
4. Click the **Save** button.
5. You can create other assessment sessions in the same way.

   ☛ *The assessment sessions created will be used to plan the assessment campaign, that is to distribute between the different assessment sessions the objects to be assessed in their context. See "Planning Assessment Campaigns", page 36.*

Viewing assessment sessions

To view assessment sessions with planned assessment dates in a Gantt chart:

- In the properties of an assessment campaign, select the **Sessions** tab and expand the **Gantt** section.

Creating and launching assessment sessions

See "Creating Assessment Sessions", page 34.

You may create an assessment session and choose to launch it:

- "**now**"
  If you choose this option, you will be able to see the assessment session being launched. This option enables to execute the following workflow transitions at the same time:
  - deploy: "Deploying Assessment Sessions", page 36
  - validate: "Validating Assessment Sessions", page 37
  - start: "Starting assessment sessions", page 38
- after saving, in batch mode ("**as soon as possible**")
- later, specifying the date and hour in UTC format ("**planned**")

Deploying Assessment Campaigns

Deploying an assessment campaign consists of indicating in advance the objects to be assessed at the level of each session of the campaign.

☛ *This step is optional. If you are not deploying the assessment campaign, go directly to "Validating Assessment Campaigns", page 36*

To deploy a campaign:

1. In the list of campaigns, click the icon of the campaign you created and select **Assessment Campaign (In Preparation) > Deploy**.
2. In the deployment window, indicate that you want to deploy the campaign now.

   ☛ *A window asks if you want to deploy the campaign:*

   - *now*
   - *as soon as possible (after dispatch)*
   - *at a later date*
3. Click **OK**.
   Assessment nodes are created.

   📖 *An assessment node comprises:*

   - *an object to assess*
   - *a respondent (or an assignment, which is a respondent associated with a particular profile)*
   - *one or several context objects (entities), if necessary*

You can now define assessment campaign scope. See "Scoping Assessment Campaigns", page 35.

Scoping Assessment Campaigns

Having deployed the assessment campaign, you must:

- define the scope, that is select the assessment nodes you want to include in your campaign.
- specify respondents.

☛ *For more details on assessment nodes, see "Deploying Assessment Campaigns", page 35*

Defining assessment campaign scope

To define campaign scope:

1. In the properties of the campaign, select the **Effective Scope** tab.
   The list of assessment nodes from your deployment appears.
2. Select the values you want to remove from the campaign and click the **Unvalidate** button.

Specifying respondents

To add or modify respondents:

❱ Select the elements that interest you and click **Set Respondent**.

Planning Assessment Campaigns

When campaign scope has been defined and assessment sessions created, you can plan the campaign.

This consists of distributing assessments between the different assessment sessions.

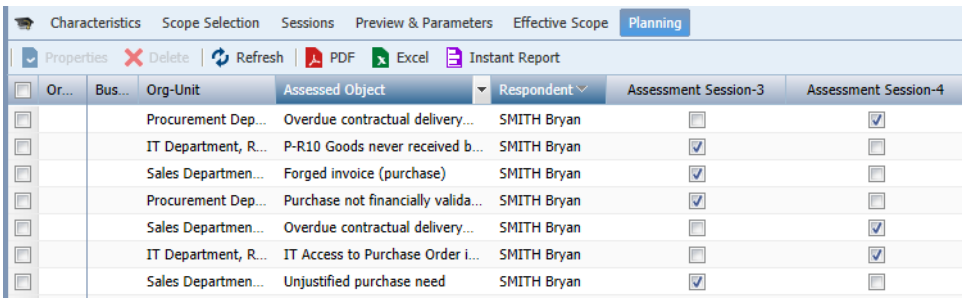
To plan the campaign:

1. In the properties of the assessment campaign, select the **Planning** tab.

   ☛ *The **Planning** tab is visible only when assessment sessions have been created.*

2. In the right pane, select the assessment sessions in which you want to assess which risk in its context (entity).

   ☛ *If you don't see the previously created assessment sessions, click the **Refresh** button.*



Or...	Bus...	Org-Unit	Assessed Object	Respondent	Assessment Session-3	Assessment Session-4
		Procurement Dep...	Overdue contractual delivery...	SMITH Bryan	☐	☑
		IT Department, R...	P-R10 Goods never received b...	SMITH Bryan	☑	☐
		Sales Departmen...	Forged invoice (purchase)	SMITH Bryan	☑	☐
		Procurement Dep...	Purchase not financially valida...	SMITH Bryan	☑	☐
		Sales Departmen...	Overdue contractual delivery...	SMITH Bryan	☐	☑
		IT Department, R...	IT Access to Purchase Order i...	SMITH Bryan	☐	☑
		Sales Departmen...	Unjustified purchase need	SMITH Bryan	☑	☐

☛ *Respondents are specified at step "Scoping Assessment Campaigns", page 35.*

Validating Assessment Campaigns

When you have planned the assessment campaign, you can validate it.

The effect of assessment campaign validation is to freeze its parameters (for example scope or planning).

To validate the campaign:

- Click the campaign icon and select **Assessment Campaign (In Preparation) > Validate**.

You can now prepare start of assessment sessions.

Deploying Assessment Sessions

Having planned and validated your campaign, you can deploy assessment sessions.

Deployment enables computing of all possible assessment nodes for the session.

> *An assessment node comprises:*
>
> - *an object to assess*
> - *a respondent (or an assignment, which is a respondent associated with a particular profile)*
> - *one or several context objects (entities), if necessary*

The session manager can then review this list.

To create the list of assessment nodes of a session:

1. Open the properties page of the campaign and select the **Sessions** tab.
2. In the **Assessment Session** section, right-click the session that interests you and select **Assessment Session (In Preparation) > Deploy**.

   > *An intermediate window asks if you want to execute the deployment now, as soon as possible (after dispatch) or at a scheduled date.*

   This operation can take several minutes.

Scoping Assessment Sessions

Having deployed the assessment session, you can:

- define the scope, that is select the assessment nodes you want to include in your session.
- specify respondents.

> *If you have defined the scope on the assessment campaign, you do not necessarily need to redefine it on the assessment session. For more details, see "Scoping Assessment Campaigns", page 35.*

Scoping the Assessment Session

To access the list of calculated assessment nodes:

- Open the properties of the assessment session and select the **Effective Scope** tab.
  From this list you can duplicate, validate, invalidate or delete elements to be assessed, and assign a respondent.

Specifying respondents

To add or modify respondents:

- In the **Effective Scope** tab of session properties, select the elements that interest you and click **Define Respondent**.

Validating Assessment Sessions

The effect of assessment session validation is to generate questionnaires, without however sending these to addressees.

Generating questionnaires

To generate questionnaires:

1. Open the properties page of the campaign and select the **Sessions** tab.
2. In the **Assessment Session** section, click the session that interests you, then **Assessment Session (To Be Validated) > Validate**.
   All questionnaires are created with status "To send". This operation can take several minutes.

You can now view questionnaires that have been generated.

Viewing generated questionnaires

To view generated questionnaires:

1. In the properties of an assessment session, select the **Questionnaires** tab.
2. Select the row relating to the assessment session and click **Display Questionnaires**.
3. Open each of the questionnaires to display the associated assessment nodes and questions.

> ☛ *If questionnaire presentation is unsatisfactory, the functional administrator can modify it at this stage.*
>
> *For more details see the **HOPEX Assessment** guide, "Assessment Template" chapter.*
>
> *In the solution, questionnaire templates are available in the tab concerning campaign management **> Preparation > Questionnaire Templates**.*
>
> ☛ *It is recommended that the assessment session be validated just before starting the session. If you validate too early, information concerning respondents could be incorrect.*

Regenerating Questionnaires

You may need to regenerate the questionnaires if for example you decide to modify respondents before starting the assessment session.

To regenerate questionnaires:

- Right-click the assessment session concerned and select **Assessment Session (To Start) > Regenerate Questionnaires**.

Starting assessment sessions

The effect of starting an assessment session is to send questionnaires to respondents.

To send questionnaires to respondents:

1. Select **Campaign Management > Campaign Management > Execution > Campaigns**.
   The list of campaigns appears in the navigation tree.
2. Select the campaign that interests you and click **Properties**.
   Properties of the campaign appear in the edit area.

3. In the **Sessions** section, click the session that interests you, then **Assessment Session (To Start) > Start**.
   The session activation page appears.
4. Click the **Save** button at top of the page.
   The assessment questionnaires are sent to respondents defined in the assessment session perimeter.

   📖 *A questionnaire proposes a list of predefined questions that can be applied to a control.*

Completing Questionnaires

The steps described here concern questionnaire respondents.

☛ *For more details on questionnaire processing steps, see "Questionnaire Generic Workflow", page 111.*

Accessing Assessment Questionnaires

After starting an assessment session, questionnaire addressees receive a notification.

To complete questionnaires:

1. Select **Home > My Desktop > My Responsibilities > My Assessment Questionnaires**.
   The list of questionnaires to be completed appears.
2. Select the questionnaire that interests you and click **Display Questionnaires**.
3. Select the questions in turn and reply to these in the lower part of the window.
4. Click **Save**.
5. Close the questionnaire display window.
6. Click the questionnaire in the questionnaires list and select **Assessment Questionnaire (To Be Completed) > Submit Answers**.

   ☛ *Questionnaires are visible from this menu as long as the assessment session is not closed. If the assessment session is closed, you can consult them in the **Questionnaires** tab of the assessment session.*

Requesting questionnaire transfer

If you receive a questionnaire in error, you can ask the session manager to transfer the questionnaire to another person.

To make a transfer request:

1. Select **Home > My Desktop > Questionnaires and Check-Lists > My Assessment Questionnaires**.

   ☛ *In some of the solutions, the corresponding menu is as follows: **Home > My Desktop > My Responsibilities > My Assessment Questionnaires**.*

2. Click the icon of a questionnaire and select **Assessment Questionnaire (To Be Completed) > Transfer Request**.
   The questionnaire passes to status "To Reassign".
   The manager is informed by e-mail and must reassign the questionnaire to another person.

   ☛ *Transfer requests are exceptional if execution campaign creation preparatory work has been correctly carried out.*

Following Up Session and Questionnaire Progress

Consulting Session Results

To consult progress of an assessment session:

1. Open the properties page of the campaign and select the **Sessions** tab.
2. Open the properties of the assessment session and select the **Reports > Follow-Up** tab.

   ☛ *For more details on this report, see "Campaign Result Tree", page 125.*

Validating assessment questionnaires

To access the list of assessment questionnaires completed by respondents:

1. In the **Risk** desktop, click **Campaign Management > Campaign Management > Follow-Up > Questionnaires Answered**.
   The list of completed questionnaires appears.
   Note that workflow status has passed to "To Be Validated".
2. Select the questionnaire that interests you and click **Display Questionnaires**.
   Content of the questionnaire appears in a new tab. You can view answers.
3. Close the questionnaire display window.
4. If you consider that the questionnaire has been correctly completed, click its icon and select **Assessment Questionnaire (To Be Validated) > Validate**.
   The questionnaire is closed and results are automatically calculated.

Asking a respondent to modify answers

If answers to a questionnaire are not suitable, you can ask the respondent to modify these.

To make a modification request:

1. Select **Campaign Management > Campaign Management > Follow-Up > Questionnaires Answered**.
2. Click the icon of a questionnaire and select **Assessment Questionnaire (To Be Validated) > Ask For Modification**.

   ☛ *The respondent can modify his/her answers. See "Completing Questionnaires", page 39.*

Reassigning questionnaires

If a respondent has made a transfer request, you must reassign the questionnaire.

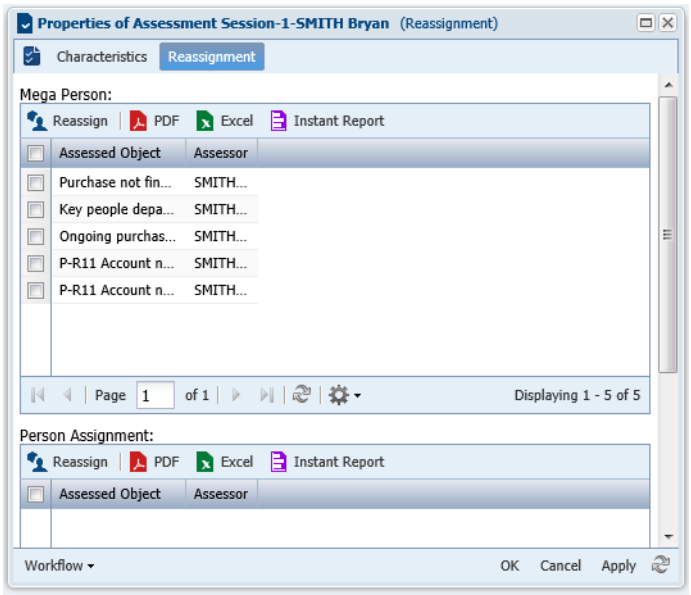
To reassign a questionnaire:

1. From the list of questionnaires sent, select a questionnaire.

   ☛ *The questionnaires are accessible from different menus according to the desktop used:*

   - *With the **MEGA** solution, you can access the questionnaires using the **Campaign Management** navigation tab.*
   - *On the assessment questionnaire laptop, the questionnaires are accessible from the **My Questionnaires** navigation pane.*

2. Open the properties dialog box of the questionnaire concerned and select the **Reassignment** tab.



   ☛ *This tab only appears when the questionnaire has "To Reassign" status.*

3. Select all nodes to be assessed and click the **Reassign** button.
4. Using the search page that opens, select a questionnaire and click **OK**.

   ☛ *If person assignments have been specified (for example, the questionnaire should be sent to a person in the context of a business role in particular), you can reassign the questionnaire in the section provided for this purpose.*

   The new respondent appears in the **Correspondent** column.

5. Select the icon of the questionnaire and select **Assessment Questionnaire (To be Reassigned) > Reassign**.

The new respondent receives an e-mail. He/she can complete the questionnaire, status of which is again "In Progress", then submit answers.

Viewing assessment campaign reports

Reports specific to assessment campaigns are available. For more details, see "Control Assessment Reports", page 125.

Closing the assessment session

You can close the session at any time.

To close an assessment session:

1. Open the properties page of the campaign and select the **Sessions** tab.
2. In the **Session** section, right-click the session that interests you and select **Close**.
   All questionnaires are automatically closed. This operation can take several minutes.

   ☛ *Results are valid only if the session is closed.*

REMEDIATING RISKS

It is particularly important to identify risk causes so that the risks themselves will be remediated and not just their symptoms. Risk assessment offers elements to select the most appropriate and cost-competitive remediation strategies.

HOPEX Enterprise Risk Management is used to specify, implement and follow up action plans defined for remediating risks.

In addition, control activities comprise policies and procedures that enable assurance that risk remediation required by management has been effectively implemented.

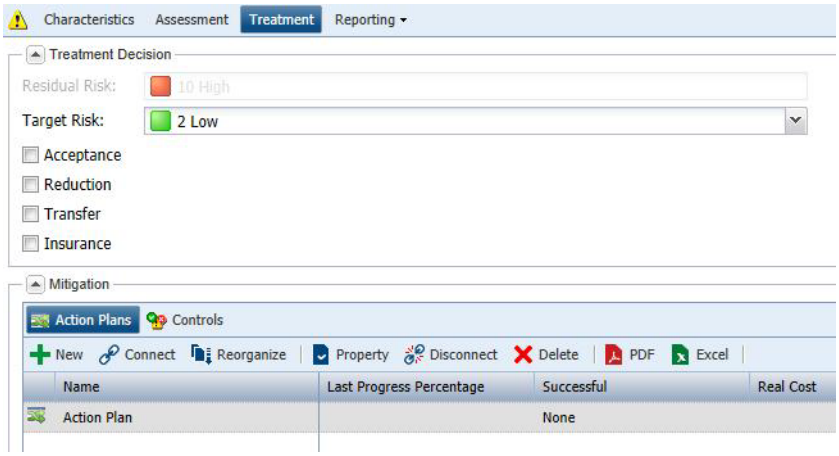
- ✓ "Describing Risk Remediation", page 44
- ✓ "Setting Up Action Plans", page 46
- ✓ "Control Policy Monitoring", page 51

DESCRIBING RISK REMEDIATION

Risk Remediation Mode

To specify risk remediation choices:

- In the properties page of a risk, select the **Remediation** tab.



Remediation modes

Various solutions that enable facing the risk are proposed.

- ***Acceptance***
  This is the strategy of risk management that consists of accepting the risk having considered its consequences. As long as no desire to remediate the risk is expressed, this strategy will not protect the organization against the risk.
- ***Reduction***
  Risk frequency can be reduced by installing additional controls, or the impact of its consequences can be reduced if the risk occurs.
- ***Transfer*** (sub-contractor)
  The risk can also be shared with other partners, in particular when they have greater skills in controlling the risk. For example, you can sub-contract a dangerous activity to a partner specialized in the particular field. In such cases, it should be noted that it is often necessary to carry out a new risk study, since the introduction of a new partner can bring additional risks.
- ***Insurance***
  Complementing all previous approaches, it is often necessary to seek assurance, in particular for risks of low frequency but with high impact. In this case, the assurer generally requests that risk prevention and reduction measures are also installed.

Analyze the different possible scenarios, weighing up their positive and negative aspects, so as to select a scenario compatible with the desired risk control level.

Depending on the solution adopted, we consider the effect of different solutions in terms of frequency and impact as well as costs and benefits.

Risk levels

The choice of remediation should be the solution that reduces **Residual Risk** to within the tolerable limit required by management.

In the **Target Risk** field, you can indicate the level of risk accepted by the organization.

Specifying Actions to be Implemented

Management draws up a set of actions matching risk levels with risk tolerance level and risk appetite for the organization.

For each risk, the selected scenario is described in detail, with the various risk factors and the controls implemented to counter them highlighted. Also specified are controls installed to warn of risks, as well as the corrective procedures to be implemented if the risks occur.

In the case of transfer to partners or assurance, we can specify contracts to be agreed with them, as well as the predicted impact on organization processes.

Implementation of prevention controls to reduce risk frequency and impact can be a solution for risk reduction.

To indicate the controls and action plans enabling risk prevention:

- In the **Remediation** tab of the risk properties page, expand the **Controls and Action Plans** section.
  - The **Action Plans** tab contains the list of action plans installed: for example for creation or improvement of a control, management of a crisis linked to occurrence of an incident, or revision of a process with a view to its improvement.

    An action plan comprises a series of actions. Its objective is to reduce the risks or events that have a negative impact on enterprise activities, or to improve efficiency of a process or organization.
  - The **Controls** tab lists controls planned for risk reduction.

    A control is a set of rules and means enabling the assurance that a legal, regulatory, internal or strategic requirement is respected.

SETTING UP ACTION PLANS

An action plan can be set up for creation and improvement of a control, management of a crisis related to occurrence of an event, or modification of a process with a view to its improvement.

> 🕮 *An action plan comprises a series of actions. Its objective is to reduce the risks or events that have a negative impact on enterprise activities, or to improve efficiency of a process or organization.*

The action plan can be created:

- in isolated then attached to different objects (risks, processes, controls, entities..)
- directly from one of these objects.

A workflow is automatically created at creation of the action plan.

Action Plan Workflows

Depending on the profile role of the person that created the action plan, two workflows are available:

- a "top-down" approach
- a "bottom-up" approach

> ☛ *Commands enabling passage from one workflow status to another are available:*
>
> - *Open action plan pop-up menu.*
> - *in the properties dialog box of an action plan, by clicking the action plan icon at top left*

"Bottom-up" approach

In a "bottom-up" approach, the action plan can be created by any user.

An approver must validate the action plan so that it can be implemented. This is the case when control assessment questionnaire respondents propose an action plan: they must submit it via the workflow.

> ☛ *For the different workflow steps, see ""Bottom-up" Action Plan Workflow", page 143*

"Top-down" approach

Within the framework of the "top-down" workflow the creator specifies:

- an approver, who sends the action plan to an owner
- an owner, who starts the action plan and terminate it one the actions have been executed.

> ☛ *For the different workflow steps, see ""Top-down" Action Plan Workflow", page 144*

Action workflow

When action plan actions have been defined, starting an action plan starts the linked actions.

When the action responsible has completed his/her actions, these can be closed. Closing the action plan automatically closes the linked actions.

☛ *See "Action Workflow", page 145.*

Creating an action plan from a risk

To create an action plan from a risk:

1. Open the properties page of a risk and select the **Remediation** tab.
2. Expand the **Controls and Action Plans** section and select the **Action Plans** tab.
3. Click the **New** button.
   The new action plan is created in the list of action plans of the risk.

   ☛ *You can specify other fields later.*

Characterizing Action Plans

☛

Before submitting the action for approval, the action plan requester can complete information on the action plan.

To update fields that characterize an action plan:

❱ Open the properties of the action plan that interests you.
In the **Characteristics** tab, the following sections appear:

- "General characteristics", page 48
- "Action plan statuses", page 48
- "Specifying action plan progress rate", page 50
- "Success factors", page 49
- "Scope", page 49
- "Milestones", page 49
- "Attachments", page 49

General characteristics

In the **Characteristics** section, you can specify action plan fields, for example:

- **Name**: action plan name.
- **Owner**: this field is specified by default by the user who created the action plan.
- **Owner Entity**: enables restriction of the list of owner entities.
- **Approver**: user responsible for validation of the action plan when all actions are completed.
- **Means**: text description of means required/desired for action plan execution.
- **Priority**: enables indication of a level. Priority can be: "Low", "Medium", "High" or "Critical".
- **Organizational Level**: final objective of plan; this can be "Global" or "Local".
- **Origin**: enables definition of the context of carrying out the action plan: "Audit", "Compliance", "Event", "Risk", "RFC" or "Others".
- **Category**: enables specification of the action undertaken, for example: "Process Improvement".
- **Nature**: enables definition of the action plan undertaken: "Preventive" or "Corrective".
- **Comment**: supplements information on the action plan and its characteristics.

Action plan statuses

- **To Send**: proposed by the action plan creator.
- **To Start**: accepted by the person designated as "approver" in the properties of an action plan.
- **Canceled**: the action plan responsible user has refused the action plan, which will not be implemented.
- **In Progress**: accepted by the action plan responsible user, actions are defined or being executed.
- **Completed**: all action plan actions have been executed. The responsible user has submitted a closing request to the approver, who can accept or refuse it.
- **Closed**: the action plan is completed and approved.

Financial assertion

- **Forecast Cost**: estimate of action plan cost expressed in **Currency**.
- **Real Cost**: action plan real cost expressed in **Currency**.
- **Forecast Cost (Man-Days)**: estimate in man-days of action plan implementation workload.
- **Real Cost (Man-Days)**: cost of action plan implementation expressed in man-days .

Success factors

In the **Success Factors** section, you can specify in text the success indicators enabling assessment of success of the action plan.

- **Key Success Factors**: text information on action plan success factors.
- **Success**: information on action plan final success. "None", "True" or "False"
- **Comments on Success**: text information on action plan results.

Scope

To position an action plan in its environment, you can associate objects with the action plan in the **Scope** section.

You can connect objects of risk, business and organizational process, control, entity or application type.

Milestones

Milestones are important dates of the action plan. You can specify these dates later.

- **Effective Begin Date** and **Planned Begin Date**
- **Effective End Date** and **Planned End Date**

Attachments

You can attach business documents to an action plan:

☛ *For more details on the use of business documents, see the **HOPEX Common Features** guide.*

Action Plan Progress Follow-Up

HOPEX Enterprise Risk Management offers the opportunity to regularly remind the action plan responsible user that he must update the progress of his action plan using a steering calendar.

Using a steering calendar

You can connect a **Steering Calendar** to the action plan if you plan to remind regularly the action plan responsible user so that action plan progress can be updated.

📖 *A steering calendar enables performing recurring actions at predefined due dates. It can be used for example for sending recurrent reminders to the person responsible for an action plan so that they can indicate progress of this element. We can also use a steering calendar to automatically trigger assessment sessions at regular intervals,...*

To specify a steering calendar:

1. Open the properties of the action plan.

2. In the **Steering Calendar** field, select for example "Action Plan - Monthly Progress Report".

   ☛ *To create a steering calendar, see technical article **HOPEX Power Studio - Steering Calendar**.*

Specifying action plan progress rate

Within the framework of a "bottom-up" workflow, once the action plan has been approved, the Risk Manager or the functional administrator can specify progress on the action plan.

The action plan progress rate can be specified if the action plan is in the status "In progress", that is it has been validated.

To indicate progress of an action plan:

1. Open the properties of the action plan and expand the **Action Plan Progress** section.
2. In the **Progress Rate** table, click **New**.
   The **Progress Rate** creation page appears.
3. Specify the **Name** of the progress rate.
4. Specify the **Updated Progress Percentage** and add a percentage **Comment**, if required.
5. Verify the **Progress Date**.
6. Specify the **Progress Assessment**:
   - Delayed
   - On Time
7. In the progress rate properties page, click **OK**.
   The progress rate appears in the list.
   The **Last Progress Percentage** and **Last Progress Percentage Comment** fields are updated.

CONTROL POLICY MONITORING

Risk identification and analysis highlighted a certain number of risks against which it is important to be protected. It is necessary to define the control activities that will prevent these risks and reduce their potential consequences.

These controls must be formally defined in order to meet regulatory requirements such as the Sarbanes-Oxley Act or Basel II agreements in the banking world.

> 🕮 *A control is a set of rules and means enabling the assurance that a legal, regulatory, internal or strategic requirement is respected.*

✓ "Managing Controls", page 51
✓ "Creating Controls", page 53

Managing Controls

In **HOPEX Enterprise Risk Management**, there are different object types linked to controls:

- Object types enabling the indication of the framework within which the control is implemented:
  - control system
  - control type
  - requirement
  - associated risk
- Object types enabling the indication of control implementation means:
  - organizational process
  - applications
- Object types enabling the indication of control implementation responsibilities.

> ☛ *Reports presenting control contextualization are available as standard. For more details, see "Control Identification", page 60.*

Accessing controls

As with risks, associated controls can be numerous. To better control their management, **HOPEX Enterprise Risk Management** proposes several means of access to the list of controls.

You can access controls via menus:

- **Risk > Risk Library > Risks > Controls > All Controls**.
- **Remediation > Controls and Action Plans > Controls > All Controls**.

Control scope

It is generally preferable to inventory existing controls before implementing new ones.

To do so, controls can be identified in various ways:

- From risks
  Certain controls are installed to meet a particular risk.
- From control type lists
  Control type lists are associated with certain regulations (eg. COBIT).
- From diagrams of existing business processes
  As during risk identification, it is possible to examine the operation of each business process step to determine the controls implemented.
- From specialist expertise
  A specialist in a particular field is often able to describe controls which are or should be implemented.
- etc.

You can define the control more precisely by indicating the control types, requirements, risks and risk factors that are attached to it.

To define control scope:

1. Select the control in the list and open its properties page,
2. Expand the **Scope** section.
   The following tabs are available:
   - **Business Process** and **Organizational Process:** enables indication of *processes* implementing the control.

     📖 *A process is a value chain providing an asset or service to an internal or external client of the enterprise. This value chain is described by a sequence of transformation activities. It is implemented by procedures.*
   - **Entities:** enables indication of entities implementing the control.

     📖 *An entity can be internal or external to the enterprise: an entity represents an organizational element of enterprise structure such as a management, department, or job function. It is defined at a level depending on the degree of detail to be provided on the organization (see org-unit type). Example: financial management, sales management, marketing department, account manager. An external entity represents an organization that exchanges flows with the enterprise, Example: customer, supplier, government office.*
   - **Risks:** enables indication of which risks are prevented by the control.
   - **Requirements**: enables indication of the regulatory or legal *requirement* the control meets.

     📖 *A requirement is a need or expectation explicitly expressed, imposed as a constraint to be met within the context of a project. This project can be a certification project or an organizational project or an information system project.*
   - **Control Type**: enables indication of the control types to which the control refers.

     📖 *A control type allows the classification of controls implemented in a company in accordance with regulatory or domain specific standards (Cobit, etc.).*
   - **Operations**
   - **Accounts**
   - **Incidents**

     📖 *An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.*

Analyzing Controls

The control types enable specification of regulations that apply to a given control.

> 🕮 *A control type allows the classification of controls implemented in a company in accordance with regulatory or domain specific standards (Cobit, etc.).*

Controls can be defined by referencing the control types defined in the risk and control system concerned.

> 🕮 *A risk and control system is a set of controls that enables the assurance of risk prevention and management, application of internal operating rules, respect of a law or regulation, or achievement of an objective as defined by company strategy.*

This control system can be defined as the implementation of a regulation within the framework of one of the enterprise business functions, such as application of an enterprise financial policy in the purchasing field.

To access control types:

- In the **Risk** desktop, select **Risk Library > Risks > Categories > Control Types**.
  A list of control types appears.

Creating Controls

To create a control:

1. In the **Risk** desktop, select **Risk Library > Risks > Controls > All Controls**.
   You obtain the list of all controls.
2. Click the **New** button.
   The control created appears in the list of controls.
3. Open the properties page of the control.
4. Specify the **Owner** of the control, who will be responsible for entering information on the new control.

HOPEX Enterprise Risk Management Reports

HOPEX Enterprise Risk Management offers risk analysis and follow-up functions.

The different report templates proposed as standard by **HOPEX Enterprise Risk Management** enable analysis of controls and risks. Report templates offer various analysis presentation possibilities.

✓ "Identification Reports", page 56
✓ "Risk Level Aggregation Reports", page 62
✓ "Follow-Up Reports", page 66
✓ "Risk Management Effectiveness", page 70
✓ "Trend Analysis", page 72

☛ *Technical documentation explaining how reports operate is available in **HOPEX Windows Front-End.***

*To access this, in the **Utilities** navigation window, expand the **Report Templates > HOPEX > Enterprise Risk Management**. Open the properties page of the concept in questions and select the **General > Documents**. tab.*

IDENTIFICATION REPORTS

Location Matrix

This matrix enables viewing of links between a list of risks and objects to which they are attached. These objects can be:

- risk type
- entity
- process
- objective

☛ *For more details on risk contextualization see "Organizing Risks", page 16.*

Access path

Reports > Identification > Distribution Matrix.

Report parameters

This consists of defining report input data.

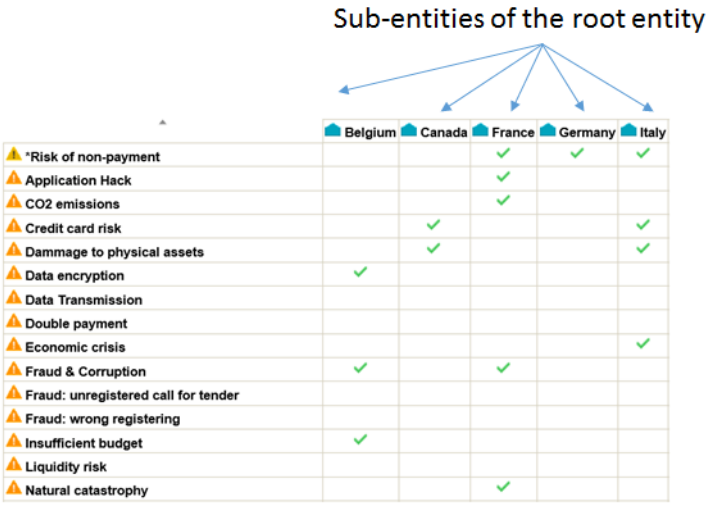
Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Inherited context	Risk type, entity, process or objective	Root (parent) of objects presented in columns. ***Mandatory***.
Risks to be distributed	List of risks (obtained from a selection related to risk type, entity, process or objective).	Risk selection criterion. ***Mandatory***.

Report example

The example below shows links between:

- a list of risks

- the list of sub-entities of the root entity specified in the ***Inherited Context***.



Risk identification

This report presents distribution of risks according to several criteria: by process, by risk type, by entity and by objective.

Access path

Reports > Identification > Risk Identification.

Report parameters

This consists of selecting risks that will be presented by specifying elements that define their scope: risk types, entities, processes or objectives.

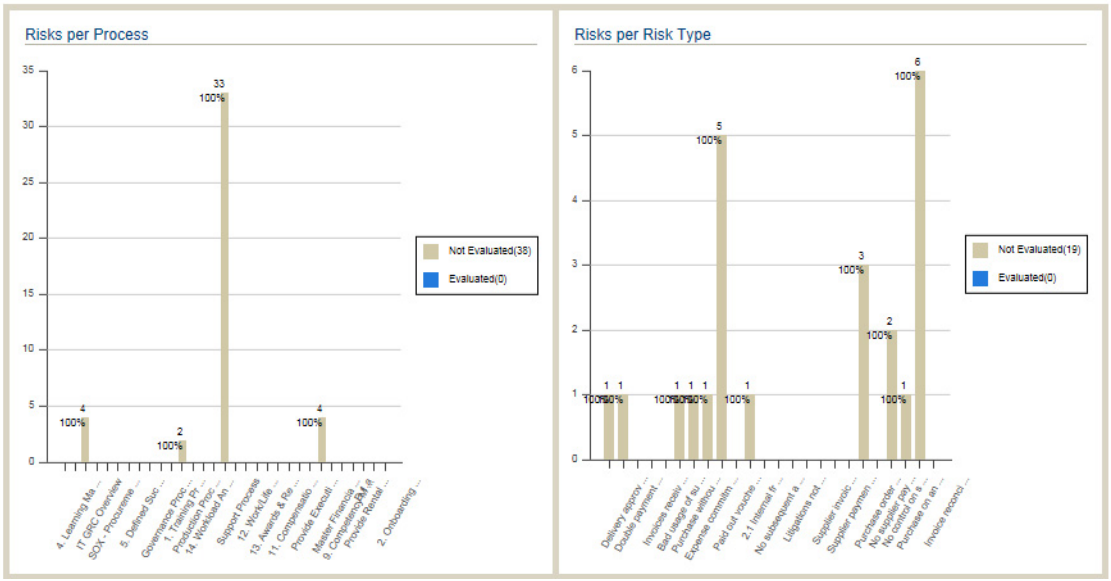
Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Scope risk type	risk type	Risk selection criterion. Not mandatory.
Scope entities	entity	Risk selection criterion. Not mandatory.
Scope processes	process	Risk selection criterion. Not mandatory.
Scope objectives	objectives	Risk selection criterion. Not mandatory.

☛ *For more details on risk contextualization see "Organizing Risks", page 16.*

Report example

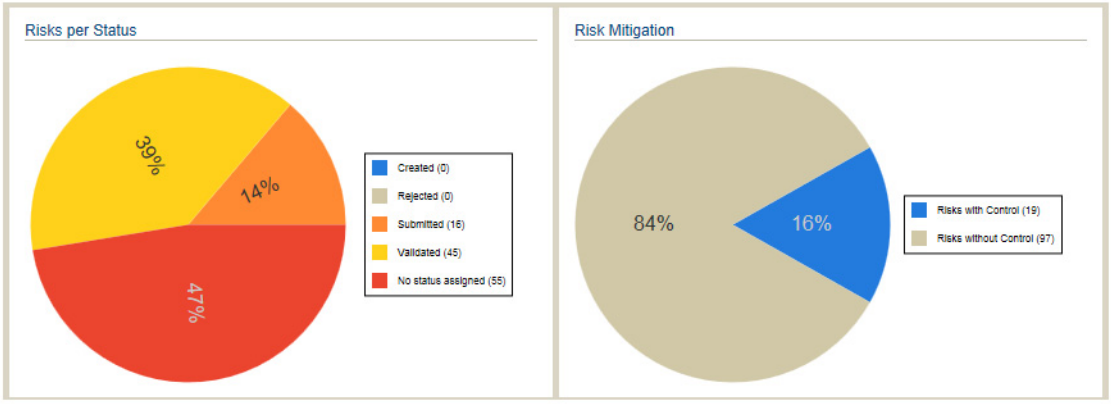
The upper part of the report presents distribution of risks on the following criteria:

- Distribution of risks by process
- Distribution of risks by risk type
- Distribution of risks by entity
- Distribution of risks by objective



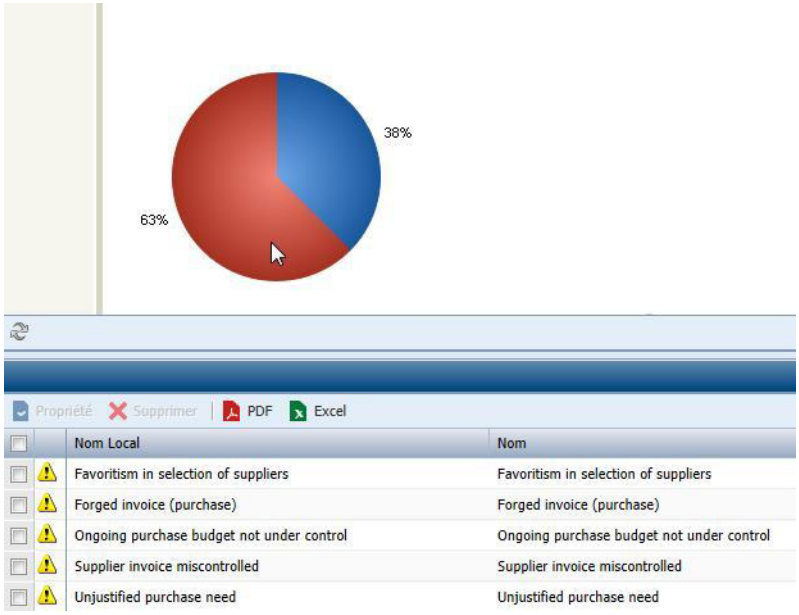
The lower part of the report presents distribution of risks on the following criteria:

- Distribution of risks by status
- Distribution of risks on which remediation has been defined
- Distribution of risks assessed or not assessed
- Number of risks created over last ten years.



To obtain a list of risks making up a sector or a barchart bar:

❱ Click the sector (or barchart bar) that interests you.



The list of risks taken into account is presented at the bottom of the edit area.

☛ *For more details on operation of instant reports, see the* ***HOPEX Common Features*** *guide.*

Control Identification

This report presents the distribution of controls according to several criteria:

- by process
- by control type
- by entity
- by objective

Its operation is identical to that of the risk identification report.

☛ *For more details on the risk identification report, see "Risk identification", page 57.*

Risks by Objective and Risk Type

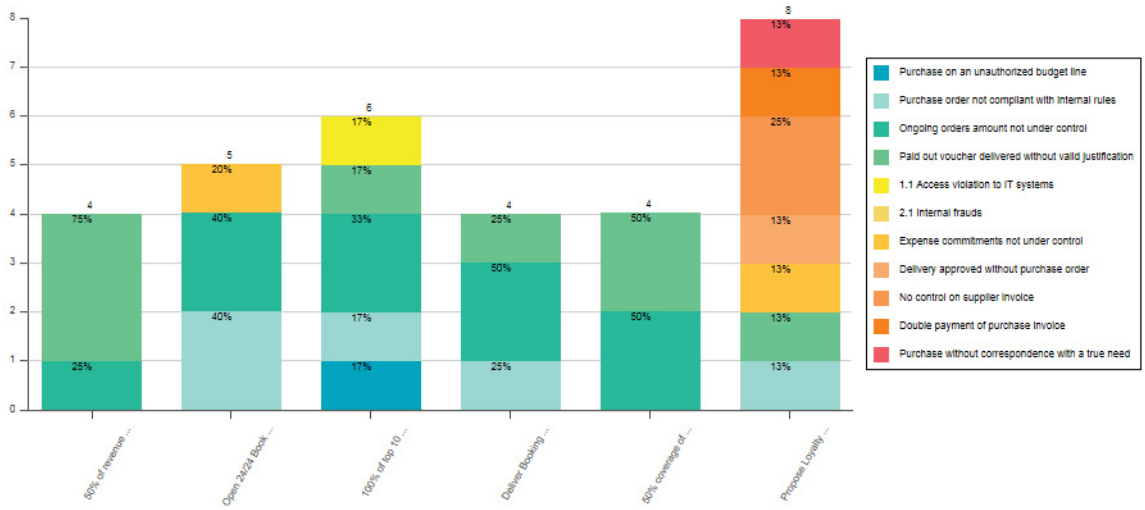
This report is presented in the form of a stacked bar chart that displays for each entity and process given as a parameter:

- on the horizontal axis: the number of risks by objective

  An objective is a goal that a company or organization wants to achieve, or is the target set by a process or an operation. An objective allows you to highlight the features in a process or operation that require improvement.

- on the vertical axis: the number of risks by risk type

  A risk type defines a risk typology standardized within the context of an organization.



Net Risk by Risk Type

This report presents in the form of a stacked bar chart:

- on the horizontal axis: the number of risks by risk type

  A risk type defines a risk typology standardized within the context of an organization.

- on the vertical axis: the number of risks by net risk level

  The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk. is the difference between the Inherent Risk and the Control Level.

Risk Level Aggregation Reports

Aggregation reports enable presentation of a summary of assessments specified on risks.

The aggregation consists of calculating an aggregated value of the values specified on each risk from assessments.

HeatMap by Entity/Risk Type/Process

This report displays distribution of risks according to different criteria:

- Risk impact related to occurrence likelihood
  - **Impact**: characterizes impact of the risk when it occurs.
  - **Likelihood**: characterizes probability that the risk will occur.
- Absolute risk related to control level
  - **Inherent Risk**: product of impact value and likelihood value. This characteristic gives an assessment of risk consequences.
  - **Control Level**: this characteristic gives an overall assessment of risk control level.

☛ *For more details on risk assessment, see "Assessments With HOPEX Enterprise Risk Management", page 21.*

Access path

Reports > Aggregation > Heatmap by Entity/Risk Type/Process

Report parameters

This consists of defining report input data.

Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Context risk type	risk type	Risk selection criterion. Not mandatory.
Context entities	entity	Risk selection criterion. Not mandatory.
Context processes	process	Risk selection criterion. Not mandatory.
Context objectives	objectives	Risk selection criterion. Not mandatory.

☛ *If you complete a risk type and and entity as a context, you get the risks connected to this risk type OR this entity (The OR operator is used here, not AND).*

Report example

In the example below, no risk has been assessed.

Impact /Likelihood

	Rare	Possible	Likely	Probable	Certain	
Very High	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	1	0	0	0	1
Very Low	0	2	0	1	0	3
Total	0	3	0	1	0	4

Control Level /Inherent Risk

	Very Low	Low	Medium	High
Very Weak	0	0	0	0
Weak	0	0	0	0
Medium	0	3	0	0
Strong	0	1	0	0
Very Strong	0	0	0	0
Total	0	4	0	0

☛ *Only the latest risk assessment values are taken into account for each Risk x Entity context.*

Aggregation Report

This report enables to sum up risk levels for an object tree (hierarchy of entities and risk types for example) as well as risk levels for each risk connected to a tree leave.

Click **Generate Aggregation** to generate aggregation data.

Access path

Reports > Aggregation > Aggregation Report

Report parameters

This consists of defining report input data.

Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Context root	The root object can be type Entity, Process or Risk Type.	Root of objects presented in rows in the report. ***Mandatory***.
Aggregation schema	Aggregation schema to be applied	***Mandatory.***
Assessed characteristics	Assessment characteristics	List of metrics presented in columns in the report. Proposed by default depending on the selected aggregation schema. ***Mandatory***.

Report example

The example below shows aggregated values of risks on entities.

1. Aggregation Results

	Avg Impact	Avg Likelihood	Avg Inherent Risk	Avg Control Level	Avg Net Risk	Max Impact	Max Likelihood	Max Inherent Risk	Max Control Level	Max Net Risk
France	Medium	Probable	Medium	Medium	High	High	Certain	Very High	Weak	Very High
Favoritism in selection of suppliers	High	Certain	Very High	Weak	Very High	High	Certain	Very High	Weak	Very High
CO2 emissions	Medium	Likely	Medium	Medium	Medium	Medium	Likely	Medium	Medium	Medium
Application Hack	Very Low	Certain	Medium	Medium	Medium	Very Low	Certain	Medium	Medium	Medium
Fraud & Corruption	Low	Possible	Low	Strong	Low	Low	Possible	Low	Strong	Low

Expanding an entity displays the aggregation of values on each of the risks connected to the entity.

	Avg Impact	Avg Likelihood	Avg Inherent Risk	Avg Control Level	Avg Net Risk	Max Impact	Max Likelihood	Max Inherent Risk	Max Control Level
MyCompany									
Subsidiaries	Medium	Likely	High	Weak	High	Very High	Certain	Very High	Very Weak
France	High	Probable	High	Weak	High	Very High	Certain	Very High	Very Weak
USA	High	Likely	High	Weak	High	Very High	Certain	Very High	Very Weak
Fraud: wrong registering	Very High	Certain	Very High	Very Weak	Very High	Very High	Certain	Very High	Very Weak
Opening of anonimous or fake saving accounts	Low	Rare	Low	Strong	Low	Low	Rare	Low	Strong
Data encryption	Low	Rare	Low	Strong	Low	Low	Rare	Low	Strong
*Risk of non-payment	Very High	Certain	Very High	Very Weak	Very High	Very High	Certain	Very High	Very Weak
Belgium	High	Possible	Medium	Weak	High	Very High	Probable	High	Very Weak
Japan	Medium	Likely	High	Weak	High	Very High	Probable	Very High	Very Weak
UK	Very Low	Probable	Low	Very Weak	High	Very Low	Probable	Low	Very Weak
Canada	Medium	Probable	High	Weak	High	Very High	Certain	Very High	Very Weak

FOLLOW-UP REPORTS

Follow-up reports concern assessments and action plans.

Action Plan Follow-Up

This report presents distribution of action plans on criteria such as the processes and entities concerned, process nature and status.

☛ *For more information on use of action plans, see "Setting Up Action Plans", page 46.*

Access path

Reports > Follow-Up > Action Plan Follow-Up

Report parameters

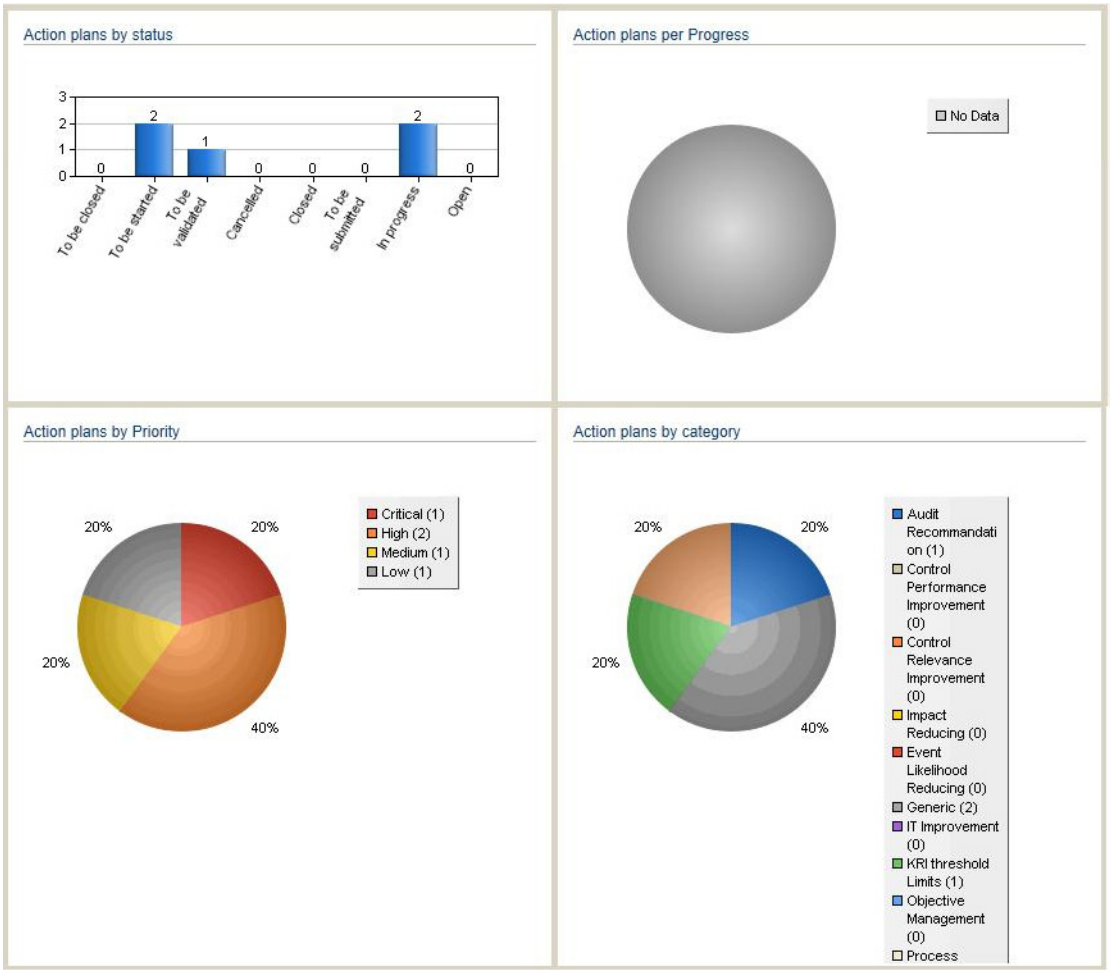
This consists of selecting action plans that will be presented in defining context elements. The action plans presented concern only those entities and processes specified in the parameters.

Parameters	Parameter type	Constraints
Begin Date	Date	Action plan selection criterion. Not mandatory.
End date	Date	Action plan selection criterion, fixed at current date.
Entities	entity	Action plan selection criterion. Not mandatory.
Business	process	Action plan selection criterion. Not mandatory.

Report example

The upper part of the report presents distribution of action plans on the following criteria:

- Distribution by nature
- Distribution by progress
- Distribution by categories
- Distribution by priorities



The lower part of the report presents distribution of action plans on the following criteria:

- Distribution by nature
- Distribution by process
- Distribution by entity

> ☛ *To obtain a list of risks making up a sector or a barchart bar:, click the sector (or barchart bar) that interests you.*

Session Statistics

This report displays the questionnaire data of a given assessment session and is used to analyze the distribution of answers.

Access path

Reports > Follow-Up > Session Statistics

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Report example

	Nb Answers	% Answers
ERM Control Level	17	100%
ERM Likelihood	17	100%
ERM Impact	17	100%
Very Low	1	5%
Low	3	17%
Production delays	1	5%
Italy, Subsidiaries, MyCompany	1	5%
Tommaso	1	5%
Economic crisis	1	5%
Dammage to physical assets	1	5%
Medium	5	29%
Production delays	1	5%
France, Subsidiaries, MyCompany	1	5%
Simon	1	5%
Favoritism in selection of suppliers	1	5%
CO2 emissions	1	5%

Result

A tree appears:

- in rows: questions/answers, together with respondents
- in columns: for each question/answer, the number of respondents
  This tree specifies who has answered what to which question.

By expanding a reply, we obtain the name of the assessor and the risks to which the reply relates.

RISK MANAGEMENT EFFECTIVENESS

Risk Reduction

This report presents evolution of the net risk between two dates in order to analyze benefits of action plans carried out.

☛ *For more details on using risk assessment, see "Assessments With HOPEX Enterprise Risk Management", page 21.*

Access path

Reports > Risk Management Effectiveness > Risk Mitigation

Report parameters

This consists of selecting risks that will be presented in defining elements that characterize their context. The risks presented concern only those entities and processes specified in the parameters.

Parameters	Parameter type	Constraints
Begin Date	Date	Begin date ***Mandatory***.
End date	Date	End date ***Mandatory***.
Entities	entity	Studied risks selection criterion. Not mandatory.
Business	process	Studied risks selection criterion. Not mandatory.

Report example

Context	Risk	AVG Net Risk 2014	Action plans	AVG Net Risk 2016
France	CO2 emissions	Medium	Implementation of CO2 sensors	Medium
France	*Risk of non-payment	Medium	*Improve control on payments	Medium
France	Natural catastrophy	High	Underwriting insurance policies	Low
France	Fraud & Corruption	Very High		Low
France	Favoritism in selection of suppliers	High		Very High
France	Application Hack	Low		Medium
France	Production delays			Low

TREND ANALYSIS

This report presents projection of the net risk over the last three years and in the coming year. It presents the average of net risk.

☛ *For more details on using risk assessment, see "Assessments With HOPEX Enterprise Risk Management", page 21.*

Access path

Reports > Trend Analysis > Trend Analysis

Report parameters

This consists in defining the context of risks presented.

Parameters	Parameter type	Constraints
Report context	risk type, entity, process, objective	Risk selection criteria presented in rows. Not mandatory.

Report example

	2014	2015	2016	Average Evolution	Action plans	Forecast 2017	Expected Evolution
Unwarranted supplier account	Medium	Very High		↗	Yes	Very High	↗
Data Transmission	Very High	Medium		↘	No	Very Low	↘
Double payment	Low	Medium		↗	No	High	↗
Favoritism in selection of suppliers	High	High	Very High	↗	No	Very High	↗
CO2 emissions	Medium	High	Medium	→	Yes	Medium	↘
Application Hack	Low	Very High	Medium	↗	No	High	↘
Natural catastrophy	High	Medium	Low	↘	Yes	Very Low	↘
Fraud & Corruption	Very High	Medium	Low	↘	No	Very Low	↘
Production delays	High	Medium	Low	↘	No	Very Low	↘
*Risk of non-payment	Medium	High	Medium	→	Yes	Medium	↘
Financial Health	Medium	High		↗	No	Very High	↗
Data encryption	Medium	High		↗	No	Very High	↗
Unauthorized spending	High	Medium		↘	No	Very Low	↘
Insufficient budget	High	Medium		↘	No	Very Low	↘
Dammage to physical assets	High	High		→	No	High	→

APPENDIX - WORKFLOWS

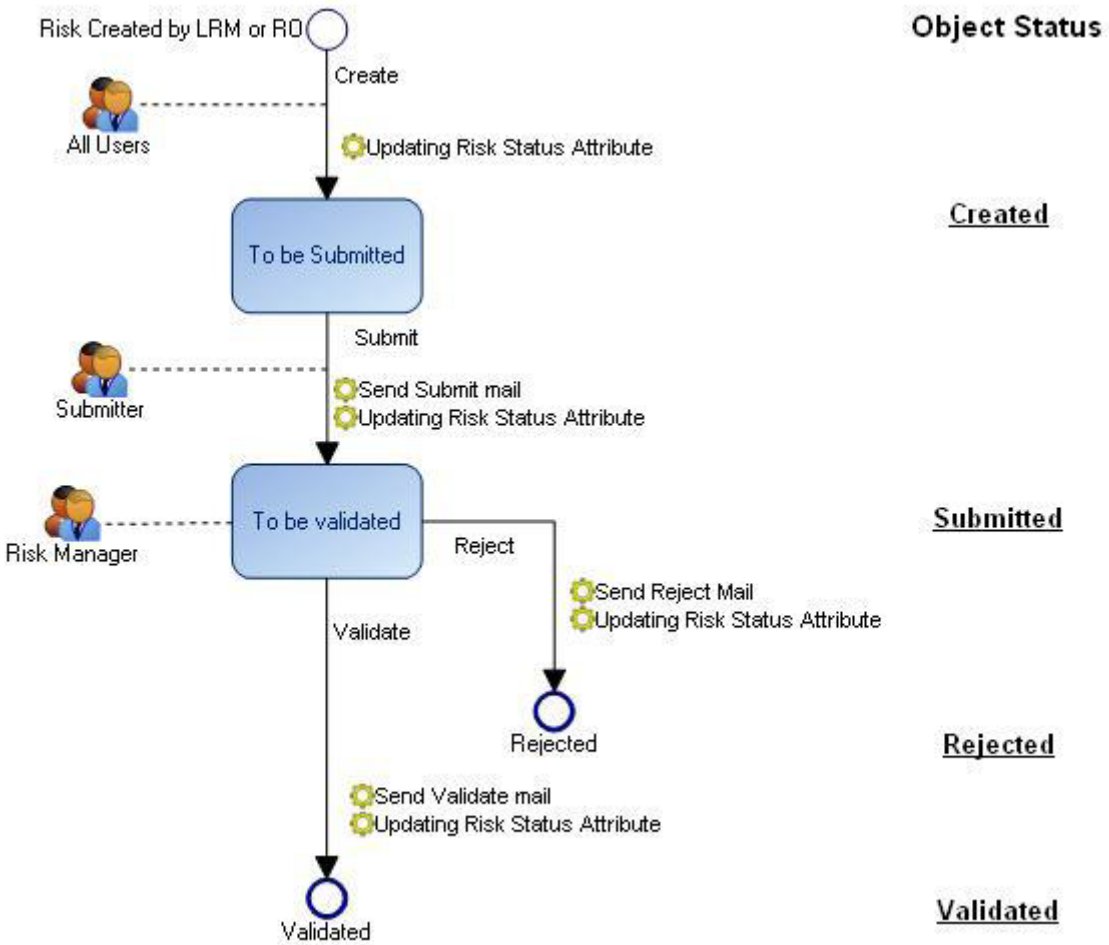
This chapter presents **HOPEX Enterprise Risk Management** workflow diagrams.

E-mails sent at each workflow transition are also listed.

✓ "Risk Workflow", page 76
✓ "Action Plan Workflow", page 78
✓ "Assessment Session Workflow", page 81
✓ "Questionnaire Workflow", page 82

RISK WORKFLOW

Risk Creation Workflow Steps



☛ *The steps in the validation process of a new risk are described in paragraph "Validating a Risk", page 15 .*

Risk Creation Workflow Mails

Request risk validation

From	Submitter
To	Risk Administrator
Subject	Risk to be validated - [Name of risk]
Content	Please validate the risk: [Name of risk]. To enter the application and perform your task, click here. Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Validate risk

From	Risk Administrator
To	Submitter
Subject	Your risk has been approved - [Name of risk]
Content	Dear Sir, Madam, The risk [Name of risk] was approved by the Risk Management department. Thank you for your collaboration Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Reject risk.

From	Risk Administrator
To	Submitter
Subject	Your risk has been rejected - [Name of risk]
Content	Dear Sir, Madam, The risk [Name of risk] was rejected by the Risk Management department. Thank you for your collaboration Comment: [Comment] This e-mail has been sent automatically by HOPEX.

ACTION PLAN WORKFLOW

Action Plan Workflow Steps

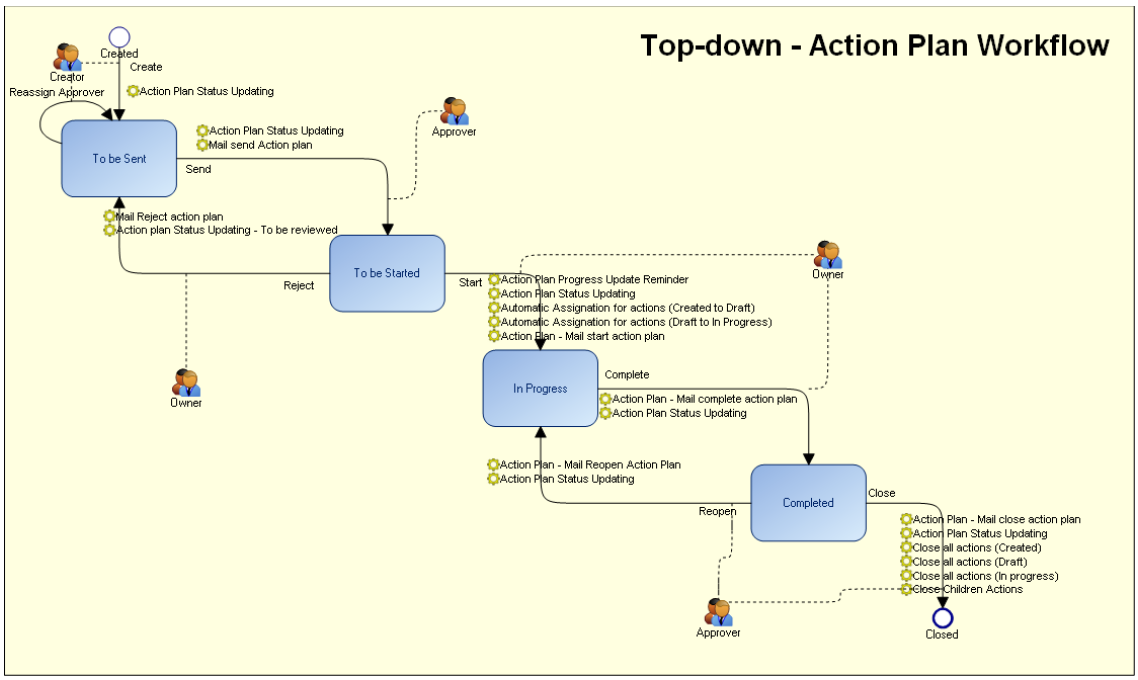
Steps in the action plan management process are described in "Setting Up Action Plans", page 46.

☛ *For more information on action plans, see the **HOPEX Collaboration Manager** guide.*

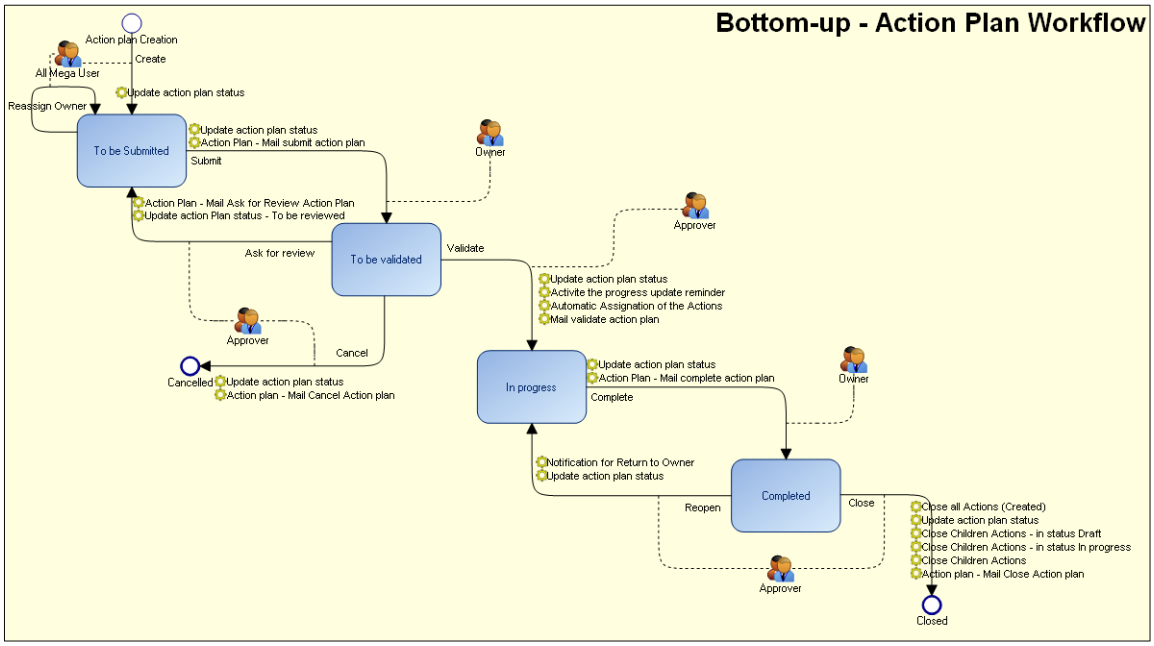
The workflow diagram introduces:

- participants
  - "Creator", who also validates action plan closure
  - "Responsible User", who is responsible for carrying out actions of the action plan
  - "Approver", who is responsible for scope covered by the action plan.
- Workflow statuses of the action plan, and planned transitions between statuses.
- Planned notifications on certain transitions.

"Top-down" Action Plan Workflow

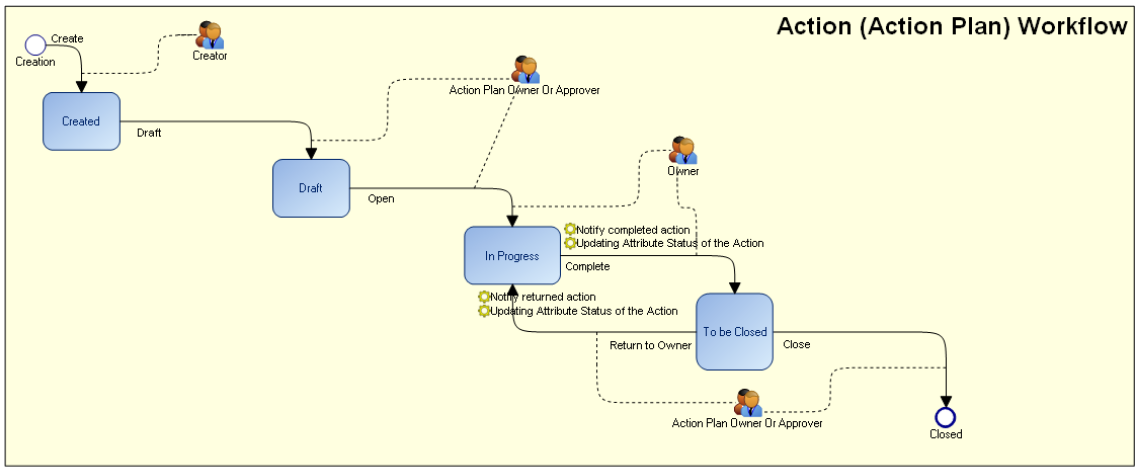


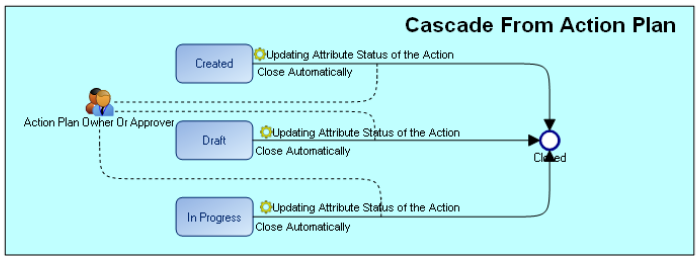
"Bottom-up" Action Plan Workflow



Action Workflow Steps

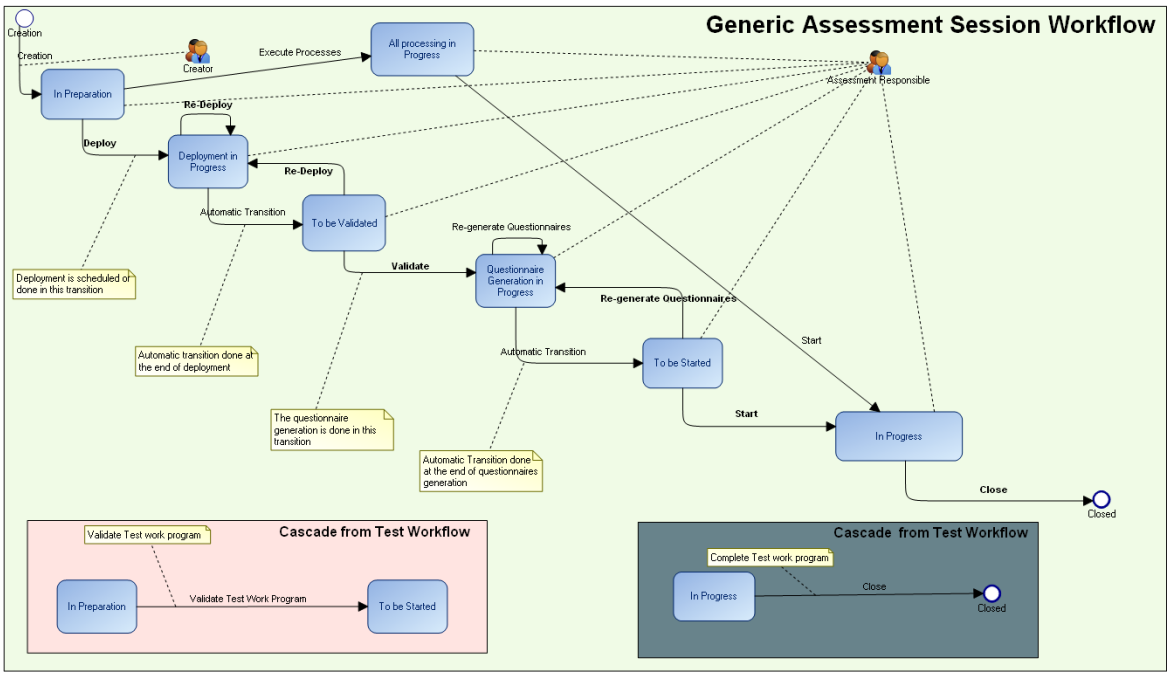
☛ *For more information on action workflows, see **HOPEX Collaboration Manager**.*


Action (Action Plan) Workflow
Create
Creation
Creator
Created
Draft
Action Plan Owner Or Approver
Draft
Open
Owner
In Progress
Notify completed action
Updating Attribute Status of the Action
Complete
Notify returned action
Updating Attribute Status of the Action
To be Closed
Return to Owner
Close
Action Plan Owner Or Approver
Closed


Cascade From Action Plan
Created
Updating Attribute Status of the Action
Close Automatically
Action Plan Owner Or Approver
Draft
Updating Attribute Status of the Action
Close Automatically
Closed
In Progress
Updating Attribute Status of the Action
Close Automatically

ASSESSMENT SESSION WORKFLOW

Assessment Session Workflow Steps

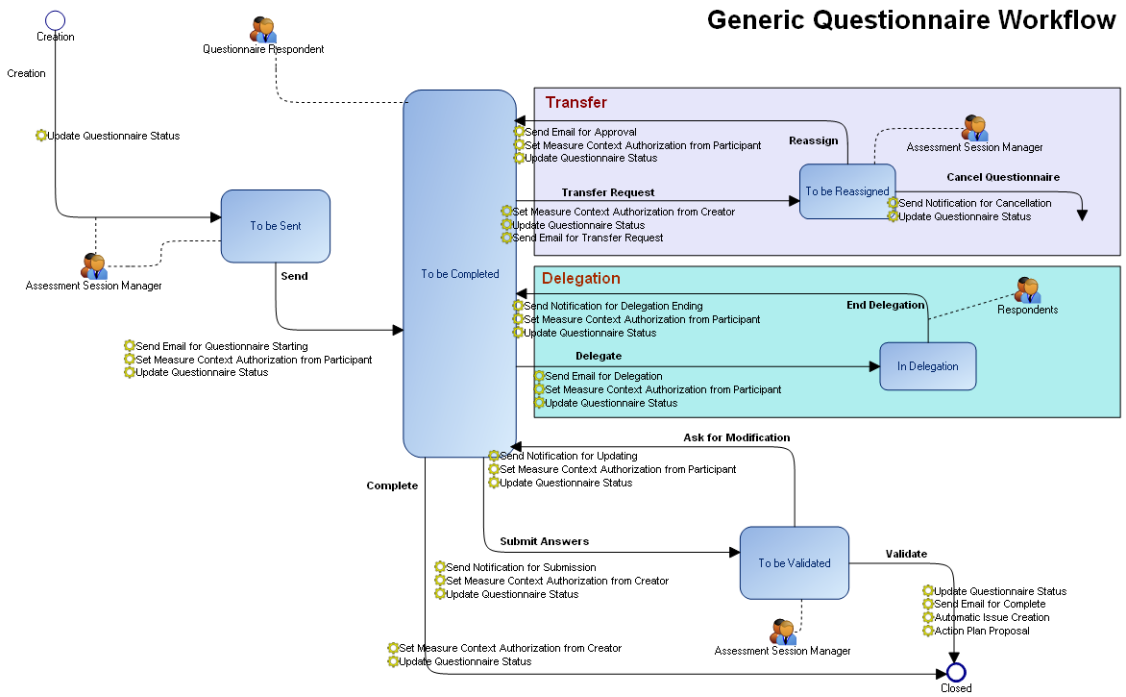


Assessment Session Workflow Notifications

No mail is sent for an assessment session. A single notification is sent by the creator to the responsible user specified for the session.

QUESTIONNAIRE WORKFLOW

Questionnaire Workflow Steps



Questionnaire Workflow Steps

Complete questionnaire

From	Session responsible user
To	Consulted on questionnaire
Subject	Assessment questionnaire to be started - [Name of questionnaire]
Content	Sir, Madam, Here is your questionnaire: [Name of questionnaire] Please complete this questionnaire and click here to send it for submission. Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Questionnaire reassigned

From	Session responsible user
To	Consulted on questionnaire
Subject	Reassign the questionnaire - [Name of questionnaire]
Content	Sir, Madam, Your request to reassign the questionnaire has been approved. Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Questionnaire to be completed by delegation

From	Consulted on questionnaire
To	Respondent
Subject	Assessment questionnaire - [Name of questionnaire]
Content	Sir, Madam, This is your questionnaire by delegation: [Name of questionnaire] Please complete this questionnaire and click here to send it for submission. Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Questionnaire validated

From	Session responsible user
To	Respondent
Subject	Answers approved - [Name of questionnaire]
Content	Sir, Madam, Your answers to the questionnaire [Name of questionnaire] have been approved. Thank you for your collaboration Comment: [Comment] This e-mail has been sent automatically by HOPEX.

Questionnaire closed

From	Session responsible user
To	Session responsible user
Subject	Questionnaire closed automatically - [Name of questionnaire]
Content	Dear Sir, Madam, Questionnaire closed automatically - [Name of questionnaire] This e-mail has been sent automatically by HOPEX.