

HOPEX IRM

HOPEX V4



M E G A
SEE THE BIGGER PICTURE

Information in this document is subject to change and does not represent a commitment on the part of MEGA International.

No part of this document may be reproduced, translated or transmitted in any form or by any means without the express written permission of MEGA International.

© MEGA International, Paris, 1996 - 2020

All rights reserved.

HOPEX is registered trademarks of MEGA International.

Windows is a registered trademark of Microsoft Corporation.

The other trademarks mentioned in this document belong to their respective owners.

HOPEX IRM Common Features



CONTENTS



Contents	1
---------------------------	----------

About the IRM Manager Desktop	7
--	----------

Accessing the IRM Manager Desktop	10
<i>Profiles used in IRM solutions</i>	<i>10</i>
<i>IRM Profiles/Solutions Summary</i>	<i>11</i>
The IRM Documentation	13

IRM Functional Administration.	15
---	-----------

Managing Teams.	16
<i>Creating controllers</i>	<i>16</i>
<i>Creating skill types</i>	<i>16</i>
<i>Creating skills</i>	<i>16</i>
<i>Creating skill levels</i>	<i>16</i>
<i>Defining skills for each user</i>	<i>17</i>
<i>Viewing skills</i>	<i>17</i>
<i>Viewing auditor assignment</i>	<i>17</i>

Managing Currencies	18
<i>Defining Central Currency.</i>	<i>18</i>
<i>Defining local currencies available to users.</i>	<i>18</i>
<i>Specifying your local currency.</i>	<i>19</i>
<i>Managing Exchange Rates</i>	<i>19</i>

Configuring Time Sheets	21
--	-----------

Managing Campaign Calendars.	22
<i>Creating calendars.</i>	<i>22</i>
<i>Creating calendar periods.</i>	<i>22</i>
<i>Connecting a calendar to an audit or test plan.</i>	<i>22</i>

Administrating Key Indicators	23
Accessing Indicator Administration Features	23
Defining Indicator Categories	23
Defining Indicator Interpretation logics	24
Defining Indicator Statuses	25
<i>Creating indicator statuses</i>	25
<i>Computation of indicator statuses</i>	25
Defining Aggregation Periods and Methods.	29
Exporting and Importing IRM Objects	30
Exporting IRM Objects	30
<i>Using the export wizard from the main menu.</i>	30
<i>Exporting IRM objects from a list</i>	30
Importing IRM Objects	31
<hr/>	
Managing your IRM Environment	33
Organization	34
Managing Entities	34
<i>Accessing organization entities.</i>	34
<i>Creating an entity.</i>	34
Managing Processes	36
<i>Accessing processes</i>	36
<i>Creating a process and sub-processes.</i>	36
<i>Specifying process scope.</i>	36
<i>Process characteristics</i>	37
Managing Business Lines	38
<i>Accessing Business Lines.</i>	38
<i>Specifying business line scope</i>	38
<i>Entering gross revenues for incident management</i>	38
Managing Applications	39
<i>Accessing applications.</i>	39
<i>Specifying application scope</i>	39
Financial Environment.	40
Accounts	40
Products	40
Gross Incomes	40
Strategic Environment	42
Risk Environment	43
Describing Risk Environment	43
Defining the Environment of a Specific Risk	43
Risk types	44
Risk factors	44
Risk consequences	45
Control Environment	46
Regulatory Environment	47
Consulting Requirements	47
Specifying Requirement Scope	47

RACI Responsibilities	48
<i>Responsibility levels</i>	48
<i>Specifying Responsibilities</i>	48
<hr/>	
Managing IRM Object Libraries	51
Managing the Regulatory Library	52
Regulatory Library Overview	52
<i>Regulatory library content</i>	52
<i>Updating the regulatory library content</i>	52
<i>Legal Inventory Objects</i>	53
Managing Regulation Frameworks	53
<i>Accessing regulation frameworks</i>	53
<i>Regulation framework characteristics</i>	54
Accessing Requirements	54
<i>Via a list</i>	54
<i>By implementing controls</i>	54
<i>Number of constrained elements</i>	54
<i>By non-compliance risks</i>	55
Creating Requirements	55
Defining Requirements	56
<i>Code</i>	56
<i>Parent requirement</i>	56
<i>Regulation framework</i>	56
<i>Priority</i>	56
<i>Analysis</i>	56
<i>Responsibilities</i>	56
<i>Scope</i>	57
<i>Sub-requirements</i>	57
<i>Milestones and Statuses</i>	58
Managing Action Plans	59
All Action Plans	59
<i>All action plans</i>	59
<i>My action plans</i>	59
<i>Delayed action plans</i>	59
<i>My delayed action plans</i>	59
Action Plan by Scope	59
<i>Action plans managing Incidents</i>	59
<i>Action plans implementing controls</i>	59
<i>Action Plans remediating issues</i>	59
<i>Action plans mitigating risks</i>	59
<hr/>	
Managing Key Indicators	61
Accessing Key Indicators	62
Accessing Key Indicators from a List	62
Accessing Key indicators by Entity	62

Defining Key Indicators	63
Creating a Key Indicator	63
Specifying the Aggregation Period and Method	63
Example of a Key Indicator	64
About Key Indicator Categories	66
Description of Key Indicator Categories	66
Relation between Indicator Category and Interpretation Logic	66
More Key Indicator Characteristics	68
Editing Key Indicator Parameters	68
Defining a Measurement Unit to be Displayed in Reports	69
Activating / Deactivating a Key Indicator	69
Specifying the Indicator Scope	69
Specifying Action Plans	70
Consulting the Key Indicator Dashboard	71
Indicator Status	71
<i>Default statuses</i>	71
<i>Information about indicator status computation</i>	72
Time To Failure	72
Indicator Freshness	73
Indicator Value	73
Defining Measurement Frequency and Notifications	74
Specifying Measurement Frequency	74
Managing User Notifications	74
Entering Periodic Key Indicator Values	74
Viewing the Indicator Graph	76
<hr/>	
Managing Assessment Campaigns	77
Introduction to Assessment by Campaign	78
<i>What is assessment?</i>	78
<i>Assessment sessions and campaigns</i>	78
<i>Questionnaire templates and questionnaires</i>	78
<i>Quotation rules</i>	79
<i>Aggregation schemas</i>	79
Accessing Assessments by Profiles	80
Accessing Assessment Templates	81
Preparing the Assessment Work Environment	83
<i>Pre-requisites to control assessment</i>	83
<i>Prerequisites to risk assessment</i>	83
Risk and Control Campaign Assessment	84
Assessment Campaign Workflow Steps	85
Creating an Assessment Campaign (with model)	86
Creating an Assessment Session	88
<i>Session creation mode</i>	88
<i>Session start options</i>	91
Deploying Assessment Campaigns	91
Defining assessment campaign scope	92
Planning Assessment Campaigns	92

Validating Assessment Campaigns	93
Deploying Assessment Sessions	93
Defining assessment session scope	94
<i>Defining assessment session scope</i>	94
<i>Specifying respondents.</i>	94
Validating Assessment Sessions	95
<i>Generating questionnaires</i>	95
<i>Viewing Generated Questionnaires.</i>	95
<i>Regenerating Questionnaires.</i>	95
Starting Assessment Sessions	95
Completing Questionnaires	96
<i>Accessing Assessment Questionnaires</i>	96
<i>Requesting questionnaire transfer</i>	96
Following Up Session and Questionnaire Progress	97
<i>Consulting Session Results</i>	97
<i>Validating Assessment Questionnaires</i>	97
<i>Asking a respondent to modify answers</i>	97
<i>Viewing assessment campaign reports</i>	97
<i>Reassigning questionnaires.</i>	97
Closing the Assessment Session	98
Consulting Assessment Results	98

IRM Reports 107

IRM Report Availability. 108

Key Indicator Reports. 109

Indicator Comparator	109
. Multi-Indicator Graph (Gauges)	110
Multi-Indicator Graph	111

Action Plan Follow-up Reports 113

Action Plan Follow-Up	113
<i>Access path.</i>	113
<i>Result</i>	113
Gantt report	114

Assessment Follow-Up Reports 116

Assessment.	116
<i>Campaign results tree</i>	116
<i>Campaign Result Matrix by Entity</i>	116
<i>Aggregation Report</i>	117
Follow-Up	117
<i>Session Follow-Up</i>	117
<i>Session Statistics.</i>	118

Regulatory Compliance Reports 120

Requirement Location Matrix	120
<i>Access path.</i>	120
<i>Parameters</i>	120
<i>Result</i>	120
Requirement Identification	121
<i>Access path.</i>	121

<i>Parameters</i>	121
<i>Results</i>	121

IRM Solution Workflows	123
Risk Workflows	124
Testing Workflows	125
Test Plan/Audit Plan Workflow	125
Test Workflow	126
Test Activity Workflow	127
Expense Sheet Workflow	128
Assessment Workflows	129
Questionnaire Workflow	129
Assessment Session Workflow	130
Action Plan Workflows	131
"Bottom-up" Action Plan Workflow	131
"Top-down" Action Plan Workflow	132
Action Workflow	133
Incident Workflow	134

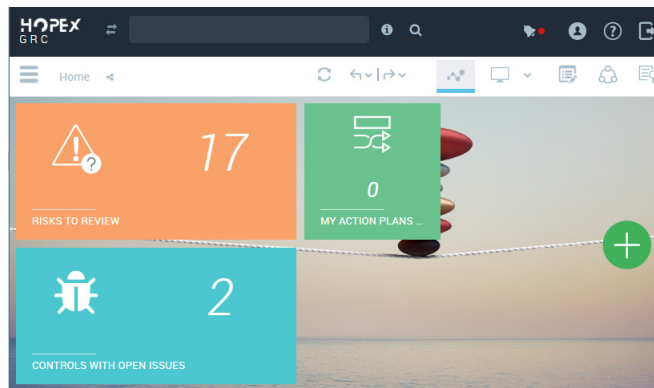
ABOUT THE IRM MANAGER DESKTOP

The HOPEX IRM (Integrated Risk Management) desktop is a central access point for risk, control, incident and audit responsible users.

It is available with the following solutions:

- **HOPEX Enterprise Risk Management,**
- **HOPEX Internal Control**
- **HOPEX LDC**
- **HOPEX Internal Audit**

The menus and features available depend on the solution(s) and profile used.



Dashboard

This section from the navigation menu enables you to add widgets specific to risk, control management and audit.

My Tasks

- **Assessment**
 - Questionnaires to Answer
 - Questionnaires to Review (to validate)
 - Assessment Sessions Due to Close
- **Execution**
 - Checklists to Complete
 - Checklists To Reassign
 - *This menu applies to **HOPEX Internal Control** only. For more information on check-lists, see [Executing controls](#).*
- **Review**
 - Incidents to Review
 - Risks to Review
 - *The objects to review are the objects which need to be validated.*
- **Audit**
 - My Work Program
 - Global Work Program
 - Past audits
 - *This section applies to **HOPEX Internal Audit** only.*
 - Past audits
- **Testing**
 - Activities
 - Vacation Requests
 - Time sheets
 - Expenses
 - *This section applies to **HOPEX Internal Control** only. For more details, see [Control Testing](#).*
- **Time and Expense Management**
 - My Vacation Requests
 - My Timesheets
 - My Expenses
 - Vacation Requests to Review
 - Expenses to Review
- **Action plans**
 - Actions to implement
 - Action plans to implement
 - Recommendations to implement
 - Late Recommendations Only (applies to **HOPEX Internal Audit**)

My Environment

See [Managing your IRM Environment](#).

Libraries

See [Managing IRM Object Libraries](#).

Key Indicators

See [Managing Key Indicators](#).

Assessment

See [Managing Assessment Campaigns](#).

Execution

See [Executing controls](#).

- This navigation menu section is available with **HOPEX Internal Control** only.

Testing

See [Control Testing](#).

- This navigation menu section is available with **HOPEX Internal Control** only.

ACCESSING THE IRM MANAGER DESKTOP

To connect to HOPEX, see **HOPEX Common Features**, "HOPEX desktop", "Accessing HOPEX (Web Front-End)".

In **HOPEX IRM**, there are profiles associated to specific activities.

The menus and commands available depend on the profile with which you are connected.

Profiles used in IRM solutions

Risk Manager

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

- identifying risks
- carrying out direct assessments
- managing assessment campaigns
- defining action plans
- analyzing and following report creation

For more details, see [Managing Risks](#).

Internal Control Director

The Internal Control Director:

- has all internal Controller rights
 - See [Internal Controller](#).
- validates campaigns
- prepares test plans
- validates action plans

For more details, see [Managing Controls](#).

Incident and Loss Administrator

The Administrator has rights on all objects and workflows.

He prepares the working environment and creates elements required for management of incidents and losses.

He manages:

- users and assignment of profiles.
- the description of the environment: org-units and organizational processes, regulatory environment, IT resources.

He can intervene in:

- declared incidents
- action plans and actions

For more details, see [Collecting Incidents](#) (HOPEX LDC).

IRM Manager

The “IRM Manager” profile is available if you have access to more than one solution among:

- **HOPEX Internal Control (IC),**
- **HOPEX Enterprise Risk Management (ERM)**
- **HOPEX LDC**
- **HOPEX Internal Audit**

It groups the following profiles (if you have the relevant solutions):

- Risk Manager
- Internal Control Director
- Incident and Loss Administrator
- Audit director

Internal Controller

The internal controller:

- defines controls
- prepares assessment campaigns
- executes tests (creates work programs, creates issues and action plans)
- validates and follows up action plans

IRM functional administrator

The IRM functional administrator has the same rights as the IRM Manager. In addition, he is offered global administration features (such as user management).

The IRM functional administrator:

- has rights on all objects and workflows.
- prepares the working environment and creates elements required for risk and control management.
- manages:
 - the description of the environment, including org-units and processes
 - the regulatory environment
 - IT resources
 - users and assignment of profiles.

IRM Profiles/Solutions Summary

<i>Solutions/ Profiles</i>	<i>ERM</i>	<i>IC</i>	<i>LDC</i>
IRM functional administrator	X	X	X
IRM Manager	X	X	X
IRM Contributor	X	X	X

Risk Manager	X		
Internal Control Director		X	
Internal Controller		X	
Incident and Loss Administrator			X

THE IRM DOCUMENTATION

The IRM documentation is structured as follows:

Features common to IRM solutions

- [Managing your IRM Environment](#)
- [Managing IRM Object Libraries](#)
 - [Managing the Regulatory Library](#)
 - [Managing Action Plans](#)
 - *For risk and control management, see **HOPEX Enterprise Risk Management** and **HOPEX Internal Control** documentations.*
- [Managing Assessment Campaigns](#)
- [Managing Key Indicators](#)
- [IRM Reports](#)
 - *For information on risks/controls/incidents, see:*
 - [Report Related to Risks.](#)
 - [Reports Related to Controls](#)
 - [Reports Related to Incidents](#)
- [IRM Solution Workflows](#)

HOPEX Internal Control

- [Managing Controls](#)
- [Executing controls](#)
- [Assessing controls](#)
- [Control Testing](#)
- [Reports Related to Controls](#)
- [Managing Issues and Action Plans](#)

HOPEX Enterprise Risk Management

- [Managing Risks](#)
- [Assessing Risks](#)
- [Report Related to Risks](#)

HOPEX LDC

- [Collecting Incidents](#)
- [Reports Related to Incidents](#)



IRM FUNCTIONAL ADMINISTRATION



So that the different participants can play their roles within the framework of an IRM (Integrated Risk Management) project, the functional administrator must first create and manage the elements required for preparation of the tasks for each of them.

- *You need to login with the "IRM functional administrator" profile for this.*

- 6 [Managing Teams](#)
- 6 [Managing Currencies](#)
- 6 [Configuring Time Sheets](#)
- 6 [Managing Campaign Calendars](#)
- 6 [Administrating Key Indicators](#)
- 6 [Exporting and Importing IRM Objects](#)

MANAGING TEAMS

You need to manage teams when using the following solutions:

- HOPEX Internal Control (tests)
- HOPEX Internal Audit (audits)

Before planning tests or audits, appropriate teams must be set up and roles and responsibilities assigned.

You must previously have defined:

- skill types
- skills list
- skill levels

Tools enable definition and display of the skills of team members.

Creating controllers

To create a controller, you must create a person and associate the "Control Tester" profile.

*- For more information on creation of users and assignment of profiles, see the chapter "Managing Users" in the **HOPEX Power Supervisor** guide.*

Creating skill types

To create a skill type:

1. In the **HOPEX IRM** desktop, select **Administration > Skill Management > All Skill Types**.
2. click **New**.
3. Enter a **Name** for the skill type, for example "Languages".
4. Click **OK**.

Creating skills

To create a skill:

1. In the IRM Functional Administrator desktop, select **Administration > Skill Management > All Skills**.
2. click **New**.
3. Enter a **Name** for the skill, for example "English".
4. Click **OK**.

The new skill is added to the list of skills.

In properties of the skill you can indicate the **Skill Type** to which it is attached, for example "Languages".

Creating skill levels

You must now create skill levels to be associated with each skill type.

To create a skill level:

1. In the **HOPEX IRM** desktop, select **Administration > Skill Management > All Skill Types**.
2. Open the properties of the skill type that interests you.
3. In the **Skill Levels** section, click **New**.
4. Enter a **Name**, for example "Beginner".
5. Click **OK**.
6. In **Skill Level Value**, enter a figure corresponding to the skill level, for example "1" for "Beginner" (while "4" could correspond with "Experienced" in our example).
 - *This figure gives a graphic view of the extent of controller skills in the test assignment page.*

Defining skills for each user

To define the skills of a user:

1. In the **Administration** navigation pane, select **Skill Management > Manage Skills with Users**.
2. Select a user and click the **Person Properties** button.
3. In the properties, select the **Skills** page.
You can specify user skills as a function of previously defined skill types and skill levels.

Viewing skills

To view the skills and skill levels available within the team:

- > In the IRM Functional Administrator desktop, select **Administration > Skill Management > Manage Users with Skills**.

MANAGING CURRENCIES

Currencies are used:

- when entering incident losses
- within the framework of tests or audits when filling in expense sheets.

Two currency types should be distinguished:

- central currency

)

- local currencyCentral currency is the currency adopted as reference currency.

) A local currency is defined for each user. By default it is the same as central currency.

Defining Central Currency

To define central currency:

1. In the Administration application (administration.exe), login to the environment of interest to you.
2. Right-click the repository and select **Options > Modify**. The repository options window opens.
3. Select the **Installation > Currency** folder. The list of currencies available as standard appears on the right.
4. In the **Monetary Symbol** field, specify the symbol of your consolidation currency, for example "\$".
5. In the **Central Currency** field, select your consolidation currency, for example "US Dollar".
6. Click **OK**.
7. Exit the Administration application.

Defining local currencies available to users

IRM functional administrator must define local currencies available to users .

(HOPEX Windows Front-End) To define the list of local currencies:

1. In the folder where **HOPEX** is installed, launch "Administration.exe" and connect with a user that has data administration authorization rights.
2. Select the environment then the repository on which you want to work.
3. Right-click the repository and select **Options**. The repository options window opens.
4. Select the **Installation > Currency** folder. The list of currencies available as standard appears on the right.
5. Then select all the currencies that will be used locally by your users.
6. Click **OK**.
7. Exit the Administration application.

(HOPEX Web Front-End) To define the list of local currencies:

1. Connect with the IRM Functional Administrator profile.

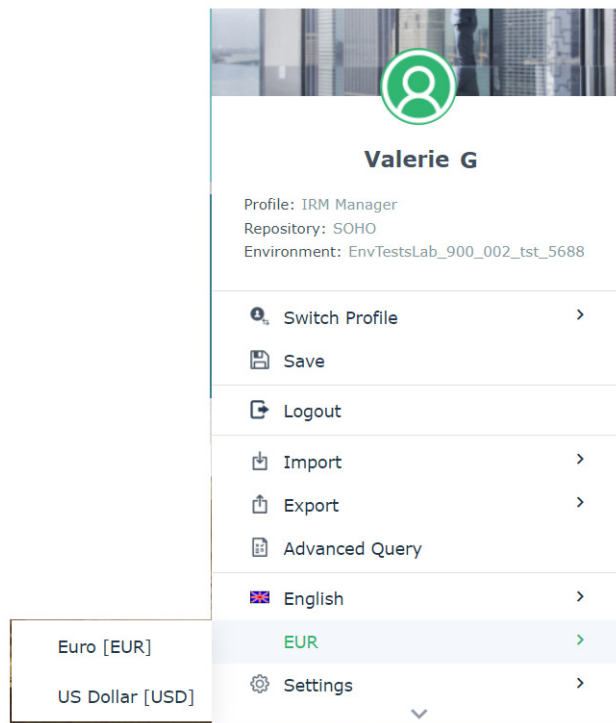
2. In the main menu, select **Parameters > Options**.
3. Select the **Installation > Currency** folder.
The list of currencies available as standard appears on the right.
4. Select all the currencies that will be used locally by your users.
5. Click **OK**.

Specifying your local currency

You can choose a local currency different from the central currency.

To modify your local currency:

- > In the main menu, select a currency as follows:



Managing Exchange Rates

To enter an exchange rate:

1. In the **HOPEX IRM** desktop, select **Administration > Tools > Exchange Rate**.
2. click **New**.

3. In the window that appears, enter:

- the **Currency Code To**.
- the **Rate** of the source currency related to the final currency.
- the **Rate Date Begin**.
 - *Several exchange rate periods can be entered for the same currency. When entering expenses, the most recent exchange rate is taken into account.*
 - *You must enter the exchange rate in both directions, for example:*
 - EUR->USD
 - USD->EUR

To view an exchange rate:

1. In the drop-down lists above the table, select the source and final currencies.
2. Click **Refresh**.
The exchange rates for the selected currency appear.

- To reverse the exchange rate, click button



CONFIGURING TIME SHEETS

Time sheets are used in the context of audits/tests.

The IRM functional administrator can configure time sheet default options.

The IRM functional administrator can define:

- number of hours worked per day
- days not worked in enterprise

To configure this data:

1. From the main menu, select **Settings > Options**.
2. In the window that appears, expand the folders **Installation > User Management**.
3. In the right pane of the window, specify:
 - the number of **Hours/Day** for each auditor.
 - *Default value is "8".*
 - days corresponding to weekend
 - *Default values are "Saturday" and "Sunday".*

A list appears. You can sort the list by skill, skill level and user by clicking the header of the corresponding column.

MANAGING CAMPAIGN CALENDARS

A campaign calendar enables planning of campaigns and their division into periods called calendar periods. Campaign calendars can also be used in reports or to plan audits or tests.

- A calendar often covers a period of one year, either a fiscal year or a calendar year. In the latter case, a calendar period can correspond to a quarter.

Creating calendars

To create a calendar:

1. In the navigation menu, click **Administration > Calendars**.
2. In the right pane of the window, click **New**.
3. Enter the **Name** of the calendar and its begin and end dates.
4. Click **OK**.

You can then define calendar periods.

Creating calendar periods

To create calendar periods:

1. Open the **Properties** of the calendar.
2. In the **Calendar Periods** section, click **New**.
3. Enter the **Name** of the calendar and its start and end dates.
4. Click **OK**.
5. Create other calendar periods in the same way.

The calendar is created. It can then be connected to an audit plan test.

Connecting a calendar to an audit or test plan

To connect a calendar to an audit or test plan:

1. From the navigation menu, click:
 - **Audits > Audit Plans**
 - **Testing > Preparation > Plans**
2. Open the properties of plan that interests you.
3. Click **Characteristics**.
4. In the **Calendar** field, click the arrow and select **List** to display the list of calendars.
5. Select the calendar to be connected.
6. Click **OK**.

ADMINISTERING KEY INDICATORS

As an IRM Functional Administrator you may need to customize the way indicators are defined (by specifying macros for Time to Failure and statuses computation, aggregation periods methods).

Key indicators are used in **HOPEX Enterprise Risk Management** and **HOPEX Internal Control**.

Accessing Indicator Administration Features

To access IRM indicator administration features:

1. Connect with the IRM Functional Administrator profile.
2. In the navigation menu, select **Administration > Indicators**.

Here you can view:

- indicator categories
 -) *An indicator category specifies how the indicator values are interpreted and how Time to Failure is computed. It also specifies how the indicator status is computed through an associated interpretation logic.*
- interpretation logics
 -) *An indicator interpretation logic contains the logic behind the computation of the indicator status, together with the list of possible statuses for the indicator. An indicator interpretation logic is linked to an indicator category.*
- indicator statuses
 -) *The indicator status is computed through an indicator interpretation logic linked to the indicator category.*
- Aggregation periods
 -) *An aggregation period is the period over which the indicator values are aggregated to compute the current indicator value and status.*
- Aggregation methods
 -) *An aggregation method is the mathematical operation carried out over the indicator aggregated values in order to compute the indicator current value and status.*

Defining Indicator Categories

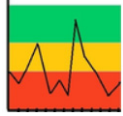
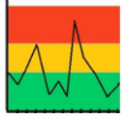
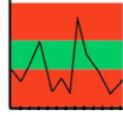
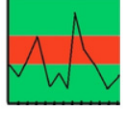
-) *An indicator category specifies how the indicator values are interpreted and how Time to Failure is computed. It also specifies how the indicator status is computed through an associated interpretation logic.*

To view indicator categories:

- > In the navigation menu, select **Administration > Indicators > Indicator categories**.

In the property page of indicator categories, you can modify the macro used to compute Time To Failure.

-) *Time to Failure is the number of estimated days before the indicator turns to "Failed" status.*
- *The macro used to compute statuses is defined on key indicator interpretation logics. For more details, see [Defining Indicator Interpretation logics](#).*

Indicator Category	Explanation	Visual Explanation
Standard	The higher threshold is used to determine the key indicator objective, thus the accepted values. All values higher than the objective are accepted.	
Reverse	The lower threshold is used to determine the key indicator objective, thus the accepted values. All values lower than the objective are accepted.	
Accepted Values	Lower and higher thresholds are used to determine the range of accepted values. Everything outside this range is rejected.	
Rejected values	Lower and higher thresholds are used to determine the range of rejected values. Everything outside this range is accepted.	

Defining Indicator Interpretation logics

-) *An indicator interpretation logic contains the logic behind the computation of the indicator status, together with the list of possible statuses for the indicator. An indicator interpretation logic is linked to an indicator category.*

You can create several indicator interpretation logics for each indicator category. It can be useful to offer several computation rules for each indicator category.

To create key indicator interpretation logics:

1. In the navigation menu, select **Administration > Indicators > Interpretation logics..**
2. click **New**.
3. In the window that opens, specify the **Indicator category** to which it is connected.
4. Specify the **Macro** used to compute indicator statuses.
 - The macro used to compute Time to Failure is defined on the Indicator category. For more details, see [Defining Indicator Categories](#).
5. In the **Indicator statuses** field, select the different statuses available for the indicators that use this interpretation logic.
6. Click **OK**.

Defining Indicator Statuses

The indicator status is computed through an indicator interpretation logic linked to the indicator category.

Creating indicator statuses

To create indicator statuses:

1. In the navigation menu, select **Administration > Indicators > Indicator statuses**.
2. Click **New**.
3. Select a **Status color** for your new status.
4. Click **OK**.

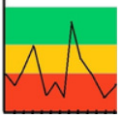
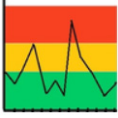
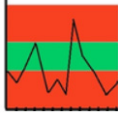
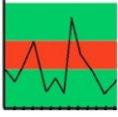
The new status you have just created will appear in the list of statuses available when creating an indicator interpretation logic. For more details, see [Defining Indicator Interpretation logics](#).

Computation of indicator statuses

The following statuses are available by default:

- Unknown
- Operational
- Warning
- Unsatisfactory
- Critical
- Failed

The indicator status is computed through an indicator interpretation logic linked to the indicator category. Hereafter are computation rules for the standard interpretation logics.

Interpretation Logics	Details	Visual representation
Standard	<p>Default rule to compute the status of "Standard" Key Indicators</p> <p>The Key Indicator is "Failed" for every value smaller than the lower threshold. For bigger values, the Key Indicator status goes from Critical to Operational, passing through Unsatisfactory and Warning.</p> <p>The status of the key indicator is Operational for values above the lower threshold + $0.75 * (\text{higher threshold} - \text{lower threshold})$.</p>	
Reverse	<p>Default rule to compute the status of Reverse Indicators.</p> <p>This rule implements the reverse logic to that used for Standard category key indicators.</p> <p>The Key Indicator is "failed" for every value higher than the higher threshold. For values below the higher threshold, the Key Indicator status goes from Critical to Operational, passing through Unsatisfactory and Warning.</p> <p>The status of the key indicator is Operational for values lower than the higher threshold - $0.75 * (\text{higher threshold} - \text{lower threshold})$.</p>	
Accepted Values	<p>Default rule to compute the status of Accepted Values indicators.</p> <p>The Key Indicator is "Failed" for every value outside the thresholds. For values within the thresholds, and as the value of the key indicator moves away from the center, the Key Indicator status goes from Operational to Critical, passing through Warning and Unsatisfactory.</p> <p>The status of the key indicator is Operational for values in the range $(\text{higher threshold} + \text{lower threshold}) / 2 \pm 0.25 * (\text{higher threshold} - \text{lower threshold})$.</p>	
Rejected values	<p>Default rule to compute status of "Rejected Values" indicators.</p> <p>The Key Indicator is in Failed status for every value within the thresholds. For values outside the thresholds, and as the value of the key indicator moves away from these thresholds, the Key Indicator status goes from Critical to Operational, passing through Unsatisfactory and Warning.</p> <p>The status of the key indicator is Operational for values above the higher threshold + $0.25 * (\text{higher threshold} - \text{lower threshold})$ (or values below the lower threshold - $0.25 * (\text{higher threshold} - \text{lower threshold})$).</p>	

Indicator status formulas

$$M = (\text{Lower Threshold} + \text{Higher Threshold}) / 2$$

$$\text{Low} = \text{Lower Threshold}$$

$$\text{High} = \text{Higher Threshold}$$

Standard category

The Key Indicator status improves as its value increases.

Status	Formula
Unknown	No available values
Failed	$KRI < \text{Low}$
Operational	$KI \geq \text{Low} + 1.5 * (\text{High} - M)$
Warning	$KI < \text{Low} + 1.5 * (\text{High} - M)$ AND $KI \geq \text{Low} + 0.75 * (\text{High} - M)$
Unsatisfactory	$KI < \text{Low} + 0.75 * (\text{High} - M)$ AND $KI \geq \text{Low} + 0.25 * (\text{High} - M)$
Critical	$KI < \text{Low} + 0.25 * (\text{High} - M)$ AND $KI \geq \text{Low}$

Accepted Values category

Status	Formula
Unknown	No available values
Failed	$KI > \text{High}$ OR $KI < \text{Low}$
Operational	$KI \geq M - 0.5 * (\text{High} - M)$ AND $KI \leq M + 0.5 * (\text{High} - M)$
Warning	$KI > M + 0.5 * (\text{High} - M)$ AND $KI \leq M + 0.75 * (\text{High} - M)$ OR $KI < M - 0.5 * (\text{High} - M)$ AND $KI \geq M - 0.75 * (\text{High} - M)$
Unsatisfactory	$KI > M + 0.75 * (\text{High} - M)$ AND $KI < M + 0.9 * (\text{High} - M)$ OR $KI < M - 0.75 * (\text{High} - M)$ AND $KI > M - 0.9 * (\text{High} - M)$
Critical	$KI > M + 0.9 * (\text{High} - M)$ AND $KI \leq \text{High}$ OR $KI < M - 0.9 * (\text{High} - M)$ AND $KI \geq \text{Low}$

Rejected Values category

Status	Formula
Unknown	No available values
Failed	$KI \leq \text{High}$ AND $KI \geq \text{Low}$
Operational	$KI < \text{Low} - 0.5 * (\text{High} - \text{M})$ OR $KI \geq \text{High} + 0.5 * (\text{High} - \text{M})$
Warning	$KI < \text{High} + 0.5 * (\text{High} - \text{M})$ AND $KI \geq \text{High} + 0.25 * (\text{High} - \text{M})$ OR $KI \geq \text{Low} - 0.5 * (\text{High} - \text{M})$ AND $KI < \text{Low} - 0.25 * (\text{High} - \text{M})$
Unsatisfactory	$KI < \text{High} + 0.25 * (\text{High} - \text{M})$ AND $KI \geq \text{High} + 0.1 * (\text{High} - \text{M})$ OR $KI \geq \text{Low} - 0.25 * (\text{High} - \text{M})$ AND $KI < \text{Low} - 0.1 * (\text{High} - \text{M})$
Critical	$KI > \text{High}$ AND $KI < \text{High} + 0.1 * (\text{High} - \text{M})$ OR $KI < \text{Low}$ AND $KI \geq \text{Low} - 0.1 * (\text{High} - \text{M})$

Reverse category

The Key Indicator status improves as its value decreases.

Status	Formula
Unknown	No available values
Failed	$KI > \text{High}$
Operational	$KI \leq \text{High} - 1.5 * (\text{High} - \text{M})$
Warning	$KI > \text{High} - 1.5 * (\text{High} - \text{M})$ AND $KI \leq \text{High} - 0.75 * (\text{High} - \text{M})$
Unsatisfactory	$KI > \text{High} - 0.75 * (\text{High} - \text{M})$ AND $KI \leq \text{High} - 0.25 * (\text{High} - \text{M})$
Critical	$KI > \text{High} - 0.25 * (\text{High} - \text{M})$ AND $KI \leq \text{High}$

Defining Aggregation Periods and Methods

The following aggregation periods are available by default:

- Weekly
- Half-monthly
- Monthly
- Quarterly
- Half-Yearly
- Yearly

) *An aggregation period is the period over which the indicator values are aggregated to compute the current indicator value and status.*

The following aggregation methods are available by default:

- Sum
- Average

) *An aggregation method is the mathematical operation carried out over the indicator aggregated values in order to compute the indicator current value and status.*

To create aggregation periods or methods:

1. In the navigation menu, select **Administration > Indicators > Aggregation Periods/Methods**.
2. click **New**.
3. In the creation wizard, connect a **Macro**.
4. Click **OK**.

EXPORTING AND IMPORTING IRM OBJECTS

HOPEX IRM enables you to exchange data via a specific import/export Excel template.

You can:

- export IRM objects in the form of an Excel file,
 - modify these objects in the generated file
 - re-import them to update the repository
- For more details, see chapter "Excel Import/Export Wizards" in the *HOPEX Common Features* guide.

Exporting IRM Objects

Using the export wizard from the main menu

To access the Excel Export Wizard and its parameters:

1. From the Main menu, select **Export > Excel**.
2. Select the "From a template" Export File Mode and click **Next**.
3. In the **Predefined Template File** select "IRM Template".
4. In the **Excel Export File** field, select the type of file you want to generate (xls orxlsx) and name this file.
5. Click Next to end-up export.


Exporting IRM objects from a list

- To be able to use the Excel template specific to IRM in object lists, you must first activate an option.

To activate the option enabling the use of the IRM-specific template in a list of objects:

1. In the main menu, select **Parameters > Options**.
2. Expand the folder **Data Exchange > Import/Export Synchronization > Tools/Third Party Formats**.
3. Select the **Excel export: Availability in listviews** check box.

To launch the Excel Export wizard from an object list:

1. Access the list of objects of interest from the object library.
 2. Select the objects you want to export.
 3. Click  to start export.
- An .xls file opens. You can save it if you wish.

Importing IRM Objects

You can manually modify the IRM objects in the previously-generated Excel One file, then re-import them into HOPEX.

- You may also download an Excel template specific to IRM solutions in the Excel import wizard.

To import objects from an Excel file to **HOPEX IRM**:

1. From the Main menu, select **Import > Excel**.
The import wizard appears in the edit window.
2. Click the **Browse** button in the **Excel Import File** section.
3. Indicate the file to be imported.
4. Click **Import**.
The wizard displays the worksheets and columns detected in the file.
If the file parameters have not been recognized by the wizard, you can enter them in this dialog box.
5. Click **Next**.
The wizard provides a report of import results.
6. To obtain a detailed report of import errors, click the **Open Report** button.
The .xls (or .xlsx) file opens indicating in color red the problem data.

P The first two lines of an Excel worksheet are reserved for file configuration. Ensure that the first two lines of the imported file remain identical to those obtained after an export.
7. Click **Finish** so that imported data will be visible in **HOPEX**.
 - To modify import parameters, click **Previous**.
 - To discard import, click **Cancel**.
 - For more details on Excel import, see [Using the Excel Import Wizard](#).

MANAGING YOUR IRM ENVIRONMENT



This section explains how to view your environment in the **HOPEX IRM** (Integrated Risk Management) desktop.

It also gives indication on how to prepare the work environment for future assessments. For more details, see [Preparing the Assessment Work Environment](#).

** Certain types of environment objects or characteristics presented can be used in some of the solutions only.*

- 3 [Organization](#)
- 3 [Financial Environment](#)
- 3 [Strategic Environment](#)
- 3 [Risk Environment](#)
- 3 [Control Environment](#)
- 3 [Regulatory Environment](#)
- 3 [RACI Responsibilities](#)

ORGANIZATION

The enterprise organization is structured around the following concepts:

- Entities: see [Managing Entities](#)
- Processes: [Managing Processes](#)
- Business lines: [Managing Business Lines](#)
- Applications: [Managing Applications](#)

Managing Entities

& 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.

Accessing organization entities

To define the list of entities of your organization, **HOPEX** allows you to create the enterprise organizational chart.

To access the different organization entities:

- â In the **HOPEX IRM** desktop, click **Environment > Organization > Entities**.

The list of entities making up the organization is displayed.

* The list of entities owned by an entity is accessible in the properties of the entity, in the **Characteristics** page, section-**Sub-Entities**.

Creating an entity

To create a new entity:

1. In the **HOPEX IRM** desktop, click **Environment > Organization > Entities**.
2. Open the properties page of the entity that owns the entity to be created.
3. In the **Sub-Entities** section, click **New**.
The entity creation page appears.
4. Enter the entity **Name** and click **OK**.
The new entity appears in the list.
5. Open the properties page of the entity created.
6. If necessary, modify the **Parent Entity**, which corresponds to the level in the tree at which you wish to create your entity.

* The **Parent Entity** field is automatically calculated according to the position of the entity in the tree.

7. Specify the **Level** of the entity in the organization:
 - "Division"
 - "Department"
 - "Service".
8. Specify the **Status**, "Active" or "Inactive" of the entity.
9. When completed, click **Save** or select another tab in the properties dialog box to carry out further modifications.

Specifying risk assessor

You need to specify the user responsible for a risk in the properties of the entity connected to this risk.

This person is called risk assessor and is in charge of filling assessment questionnaires.

To specify the risk assessor on an entity:

1. In the navigation menu, select **Environment > Organization > Entities**.
2. Open the properties of an entity.
3. In the **Risk Assessor** field, select the user in charge of assessing the risk.

* You must specify this field in the context of risk assessment by campaigns with **HOPEX IRM**.

Scoping an entity

An entity can intervene in the framework of a process. It can be broken down hierarchically.

An entity can be connected to different component types.

- **Entities**: you can specify the entity responsible for a service or management, as well as functional dependency between two entities.
- **Business Processes** and **Organizational Processes** for which the entity intervenes. For more details, see [Managing Processes](#).
- **Risks**, whose management is assigned to the entity. For more details, see [Managing Risks](#).
- **Controls**, whose management is assigned to the entity. For more details, see [Managing Controls](#).
- **Objectives and Requirements** assigned to the entity. For more details, see [Strategic Environment](#) and [Regulatory Environment](#).

* Certain key documents, such as strategic plans, the business plan, annual reports, economic analyses and other relevant documentation related to the organization and its aims may be consulted to define its **objectives** and **requirements**.

- **Business Lines** for which the entity intervenes. For more details, see [Managing Business Lines](#).
- **Regulation Articles**

Regulation articles are available only with **HOPEX UCF**. For more information, see [Using HOPEX UCF](#).

* Depending on your rights, you may also see the **Action Plan** or incidents owned by the entity.

Managing Processes

Available process types are:

- business processes

& A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.

- organizational process

& An organizational process describes how to implement all or part of the process required to make a product or handle a flow.

The type is requested at creation of the process. The two types are distinguished by different icons in the trees and lists.

Accessing processes

To access the business processes tree:

- â In the **HOPEX IRM** desktop, click **Environment > Organization > Processes**.

Columns display:

- The total of sub-processes, entities and business lines performing processes
- The applications involved in each process.

Creating a process and sub-processes

To create a process:

- â Right-click the "Process" folder and select **New**.

To create a sub-process:

- â Right-click a process from the tree and select **New**.

To modify the list of sub-processes of a given process:

- â Open the process property pages and click **Characteristics > Sub-processes**.

If you expand the folder of a process, you can display the sub-processes owned by the current process.

Specifying process scope

To view/modify the list of entities or business lines performing a process:

- â Open the properties of the process and select:
 - **Characteristics > Scope > Entities**, or
 - **Characteristics > Scope > Business lines**

To view or modify the list of applications supporting a process:

- â Open the properties of the process and select **Characteristics > IT > Applications**.

Process characteristics

To access characteristics of a process:

- â Open the **Characteristics** page of the process properties.

Business process control is the responsibility of persons with different functions.

- the **Owner** is responsible for global operation of the process in terms of effectiveness, profitability and security,
- the **Responsible** person takes decisions concerning evolution of the process, and informs on progress,
- the **Risk Assessor** is consulted when an action relating to risks is planned or executed on the process.

To specify business process control responsibilities:

1. In the **Characteristics** page of a business process properties, position the mouse on the **Owner** field for example and enter the first letters of the name.
2. Click the arrow at the right of the field and select **List Persons**.
The name of the selected person appears in the field.

& A person is defined by his/her name and e-mail. The person can access an application after assignment of a connection identifier. One or several business roles can also be assigned.

Scope section of a process

A process can be linked to different component types.

- **Entities** that intervene in the process framework. For more details, see [Managing Entities](#).
- **Business Lines** that use the process services. For more details, see [Managing Business Lines](#).
- **Risks** that relate to the process. For more details, see [Managing Risks](#).
- **Controls** that relate to the process. For more details, see [Managing Controls](#).
- **Incidents**
- **Action Plans**
- **Regulations** For more details, see [Managing the Regulatory Library](#).
- **Control Systems**

& A control system is a set of controls that ensure risk prevention and management, application of internal operating rules, respect a law or regulation, or work towards achievement of an objective as defined by company strategy. Examples: quality control system, management control system, internal audit system.

- **Regulation Articles**

Regulation articles are available only with **HOPEX UCF**. For more information, see [Using HOPEX UCF](#).

Other sections of a process

The properties page of a process presents the following sections:

- **RACI**: to present the persons responsible for the process. For more details, see [RACI Responsibilities](#).
- **Objectives and Requirements**: for more details, see [Strategic Environment](#)
- **IT**: IT resources are made available to processes to execute the operations necessary for their implementation. For more details, see [Managing Applications](#).

Managing Business Lines

& A business line is a skill or grouping of skills of interest for the enterprise. It corresponds for example to major product segments, to distribution channels or to business activities.

The business lines overview presents the different businesses carried out by the enterprise.

Accessing Business Lines

To access the different organization business lines:

- â In the **HOPEX IRM** desktop, click **Environment > Organization > Business Lines**.

From this page you can view trees of business lines of the organization, consult their properties and create new objects.

** The list of business lines owned by a business line is accessible in the properties page of the business line, section **Sub-Business Lines**.*

To access characteristics of a business line:

- â Expand the **Characteristics** section of the properties pane of the business line that interests you.

Specifying business line scope

A business line can be implemented by:

- **Org-Units**: for more details, see [Managing Entities](#).
- **Applications**: for more details, see [Managing Applications](#).
- **Risks**

A business line can be connected to different component types by, for example, **Business Processes** and **Organizational Processes**, which use services of the business line. For more details, see [Managing Processes](#).

Entering gross revenues for incident management

The **HOPEX IRM** desktop enables the Incident and Loss Administrator to enter gross incomes for the organization so as to perform a BIA analysis.

** For more details, see [Gross Incomes](#).*

Gross Incomes are linked to business lines.

Managing Applications

& An application is a set of software tools coherent from a software development viewpoint.

Accessing applications

To access applications:

- â In the **HOPEX IRM** desktop, click **Environment > Organization > Applications**.

Columns display:

- The number of sub-applications
- The number of supported business processes
- The number of business lines which depend on each application

Specifying application scope

You can indicate which IT application is available for an entity or used in execution of a process.

To view / edit the list of business processes supported or business lines:

- â Open the properties of the application and select:
 - **Characteristics > Scope > Business process**, or
 - **Characteristics > Scope > Business lines**

You can attach numerous others objects in the **Scope** section of the application properties:

- Risk
- Control
- Control System
- Action plan
- Incidents

* Implemented Functionalities can be accessed in read-only mode only.

FINANCIAL ENVIRONMENT

To access components of the financial environment:

- â In the navigation menu, click **Environment > Financial**.

Accounts

This tile displays all the accounts to be monitored withing the framework of SOX compliance.

Account characteristics are as follows:

- **Account type**
The profits and losses account presents a description of profits and losses of the enterprise during the fiscal period. You can specify if the account is:
 - "Profits"
 - "Losses"
- **Total Value**: you can enter a total for this account.
 - * *An order of magnitude is sufficient.*
- **Status**
 - "Open": the account is active
 - "Closed": the account is inactive
 - * *The account can comprise sub-accounts.*
 - * *You can connect an entity to an account in the **Scope** section of the account.*

Products

A product represents commodities offered for sale, either goods or merchandise produced as the result of manufacturing, or a service, i.e., work done by one person or group that benefits another.

Gross Incomes

Gross revenues are entered by the Incident and Loss Administrator for each business line and are used within the framework of the BIA approach (Basel II).

Gross Incomes are linked to business lines.

- * *For more details, see [BIA Approach](#).*

To create a gross income:

1. Click **Environment > Financial > Gross Incomes**.
2. Click **New** and open the property page of the income created.

3. Select a **Business Line** in the corresponding field.
4. Select a **Begin Date** and **Date Date** to define a time period.
5. Enter a **Revenue Amount**.

STRATEGIC ENVIRONMENT

The hierarchy of strategic objectives in your organization appears in a tree.

& 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.

To access the tree of objectives within your organization:

â In the navigation menu, select **Environment > Strategy**.

To create an objective:

â Right-click the "Objectives" folder or on an objective and select **New**.

Depending on the solution you user, the following information is displayed:

- (**HOPEX Internal Control**) the number of controls contributing to objective achievement.
- (HOPEX Enterprise Risk Management) the number of risks that possibly hinder objective achievement.

RISK ENVIRONMENT

To analyze a risk, it is necessary to take into account all the elements of the environment.

Describing Risk Environment

To describe the objects which make up the environment of a risk:

- â In the **HOPEX IRM** desktop, click **Environment > Environment > Risks**.

You can define:

- Risk Types
 - & A risk type defines a risk typology standardized within the context of an organization.
- Risk factors
 - & A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...
- Risk consequences
 - & A risk consequence can be positive or negative. It is associated with a type, which enables its characterization, for example: image, environment, employees.

Defining the Environment of a Specific Risk

To define the environment for a specific risk:

- â In the **Characteristics** page of the property window of a risk, expand the **Analysis** section.

A risk is characterized by:

- **Risk types**
 - & A risk type defines a risk typology standardized within the context of an organization.
- **Risk factors**
 - & A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of

involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...

- **Risk consequences**

& A risk consequence can be positive or negative. It is associated with a type, which enables its characterization, for example: image, environment, employees.

- **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.

- **Control systems**

& A control system is a set of controls that ensure risk prevention and management, application of internal operating rules, respect a law or regulation, or work towards achievement of an objective as defined by company strategy. Examples: quality control system, management control system, internal audit system.

- **Associated Risks**

Risk types

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

A risk type enables risk characterization. For example, a risk type can be regulatory, legal, technical, etc.

To create your own risk types:

1. In the **HOPEX IRM** desktop, click **Environment > Risks > Risk types**.
2. In the pop-up menu of the "Risk Type" folder, select **New**.
3. Enter the name of the risk type and click **OK**.

The new risk type appears in the navigator menu tree.

* Similarly, you can create a sub-risk type from a risk type.

Risk factors

Many risk factors are defined within the framework of international, national or inter-professional regulations, or within the enterprise itself.

& A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...

With each risk, you can associate one or more risk factors, sources of risks that have intrinsic potential to endanger organization operation. For example, dangerous chemical products, competitors, governments, etc.

Risk consequences

To define consequences associated with a risk:

- â In the risk page, **Analysis** section, **Risk Consequences** tab, click **New**.
The consequence creation page appears.

- * *Since a risk consequence can relate only to a single risk, the **Risk** field is already entered with the current risk.*

The consequence created appears in the list of consequences associated with the risk.

CONTROL ENVIRONMENT

To describe control environment:

- â In the **HOPEX IRM** desktop, click **Environment > Controls**.

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

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

To view sub-control types and controls:

- â Click the + sign of the control type of interest.

For each control type, the sum of sub-control types and controls is computed.

To remove and/or connect controls from/to a control type:

- â Open the control type properties and select **Characteristics > Controls**.

REGULATORY ENVIRONMENT

* To specify the legal inventory, see [Managing the Regulatory Library](#).

The legal inventory constitutes the regulation framework repository applying to an organization. The regulation framework comprises:

- regulations
 - & A regulation or policy is a set of directives, compulsory or not, defined by a government in a law, by standard bodies as "best practices" or as an internal policy in an organization.
- requirements
 - & 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.

Consulting Requirements

To consult requirements:

- â In the **HOPEX IRM** desktop, click **Environment > Regulations**.

You can use this tree to view:

- Whether requirements apply to the organization
- Which controls implement these requirements

Columns display:

- The number of sub-requirements
- The number of impacted entities, processes and applications.

Specifying Requirement Scope

To connect a constrained element to a requirement:

1. In the **HOPEX IRM** desktop, click **Environment > Regulations**.
2. Open the requirement properties and select the **Characteristics > Scope**.

For each requirement, the number of immediate requirements and constrained elements appear.

RACI RESPONSIBILITIES

HOPEX solutions enable definition of responsible users for some of the objects via the RACI matrix.

* *RACI is the acronym of Responsible, Accountable, Consulted, Informed.*

Responsibility levels

The proposed responsibility levels are as follows:

Responsibility	Meaning
Responsible	Persons responsible for execution of required actions.
Accountable	Persons reporting on progress of planned actions and making decisions. There is only one "Accountable" for each action.
Consulted	Persons consulted as first priority before an action or decision.
Informed	Must be informed after an action or decision.

HOPEX enables specification of the responsibility level of the various persons:

- on a business or organizational process,
- on a risk,
- on a control.

Specifying Responsibilities

One or various persons can take responsibility for a specific object.

To specify the persons concerned by a specific object:

3. In the object properties page, expand the **RACI** section.
4. Connect the persons or person assignments in each of the following tabs:
 - **Responsible**
 - **Accountable**
 - **Consulted**
 - **Informed.**

* *In some solutions, RACI information can be redundant with roles defined in the object property dialog box or can supplement them.*

For example, in **HOPEX Enterprise Risk Management**, the process responsible user can be specified directly in the **Responsible** field of the process property dialog box and not in the RACI section. In this case, it is important to specify one responsible user only.

MANAGING IRM OBJECT LIBRARIES



The **HOPEX IRM** (Integrated Risk Management) desktop enables you to manage risk, control, regulatory requirement, incident and action plan libraries.

The following section describes the libraries used across all solutions.

- [Managing the Regulatory Library](#)
- [Managing Action Plans](#)
- [Managing Key Indicators](#)

Risks and control libraries are described in the **HOPEX Enterprise Risk Management** and **HOPEX Internal Control** documentations respectively:

- [Managing Risks](#)
- [Managing Controls](#)
 - *To consult elements which apply to your organization, see [Managing your IRM Environment](#).*

MANAGING THE REGULATORY LIBRARY

The purpose of the regulatory library is to manage the regulation framework applying to an organization.

HOPEX enables creation of this regulatory library, generally derived from an external source (for example, the American Bankers Association).

Regulations and requirements can be organized by process, entity and risk.

Regulatory Library Overview

Regulatory library content

The regulatory library constitutes the regulation framework repository applying to an organization. It consists of:

- regulation frameworks
 -) *A regulation framework is a set of directives, compulsory or not, defined by a government in a law, by standard bodies as "best practices" or as an internal policy in an organization.*
 - For more details, see [Managing Regulation Frameworks](#).
- requirements
 -) *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.*
 - For more details, see [Defining Requirements](#).

Updating the regulatory library content

The regulatory library is generally supplied by external sources.

The functional administrator imports the following on a regular basis:

- regulation frameworks
- requirements (first and second level)

To execute import:

- > In the main Menu, select **Import**.
 - For more details on the import tool, see **HOPEX Common Features** guide, "Exchanging Data with Excel".

Legal Inventory Objects

Legal Inventory Context

Regulation Frameworks and requirements can be organized by:

- process (business or organizational)
- entity
- risk

Regulation frameworks and requirements can be:

- connected to risks and to all levels of processes and entities
- connected to several processes, entities and risks

Legal Inventory Hierarchy

Legal inventory repository objects are managed as follows:



The GRC functional administrator manages the hierarchy of the legal inventory and can connect regulations and requirements to processes, entities and risks.

Managing Regulation Frameworks

) A regulation framework is a set of directives, compulsory or not, defined by a government in a law, by standard bodies as "best practices" or as an internal policy in an organization.

Accessing regulation frameworks

To access regulation frameworks:

- > In the **HOPEX IRM** desktop, select **My environment > Regulation Frameworks**.

A tree showing regulation frameworks appears.

Regulation framework characteristics

You can specify:

- **Code:** enables unique identification of the regulation
- **Application Begin Date**
- **Application End Date**

Accessing Requirements

) *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.*

Via a list

To access all requirements in the form of a list:

- > In the **HOPEX IRM** desktop, click **Libraries > Regulatory Library > All Requirements**.

From the drop-down list you can select:

- All Requirements
- High Priority Requirements

By implementing controls

To view requirements implemented by Controls:

- > In the **HOPEX IRM** desktop, click **Libraries > Regulatory Library > By Implementing Controls**.

Drop-down lists display:

- Requirements implemented by Controls
- Requirements not implemented by Controls

Number of constrained elements

To view requirements constraining the organization:

- > In the **HOPEX IRM** desktop, click **Libraries > Regulation Library > By Constrained Elements**.

The list displays the number of elements to which the requirements apply (processes, entities, applications).

You can also display requirements not constraining the organization through the drop-down list.

By non-compliance risks

This list displays requirements showing non-compliance risks.

- > In the **HOPEX IRM** desktop , click **Libraries > Regulation Library > By Non-Compliance**.

The following lists are displayed:

Requirements with non-compliance risks

Lists requirements linked to risks

Requirements with deficient controls

Lists requirements linked to implementing controls having open issues

Requirements with Unexecuted Controls

Lists requirements implemented by one or more controls with an execution rate below 90%.

By Incidents Against Constrained Elements

Lists requirements with constrained elements at Risk where incidents occurred.

The columns display:

- the number of incidents against the elements constrained by the requirement
 - *This concerns open incidents.*
- the date of the last incident occurrence
- the number elements constrained by the requirement

Creating Requirements

The GRC functional administrator can create requirements.

) *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.*

To create a requirement:

1. In the **HOPEX IRM** desktop, click **Libraries > Regulation Library > By Regulatory Framework**.
2. In the tree which appears, right-click the regulation framework and select **New**.
You can now specify the various characteristics from the properties window.
 - *For more details, see [Defining Requirements](#).*

Defining Requirements

Different sections are available in the properties of a requirement.

- To access requirements, see [Accessing Requirements](#).

Code

The code enables unique identification of the requirement.

Parent requirement

This is the requirement to which this requirement is attached.

Regulation framework

A regulation or policy is a set of directives, compulsory or not, defined by a government in a law, by standard bodies as "best practices" or as an internal policy in an organization.

- For more details on regulations, see [Managing Regulation Frameworks](#).

Priority

Priority can be:

- Low
- Medium
- High

Analysis

- Risk factors

) A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...

- Event type Basel (level 1)
- Event type Basel (level 2)

Responsibilities

HOPEX IRM enables definition of responsibilities of each participant related to a requirement via the RACI matrix.

- For more details, see [RACI Responsibilities](#).

Scope

The **Scope** section of requirement properties enables connection of requirements to other objects:

- Business processes
 -) *A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.*
- Organizational processes
 -) *An organizational process describes how to implement all or part of the process required to make a product or handle a flow.*
- Entities
 -) *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
 -) *A risk is a hazard of greater or lesser probability to which an organization is exposed.*
- Risk types
 -) *A risk type defines a risk typology standardized within the context of an organization.*
- Applications
 -) *An application is a set of software tools coherent from a software development viewpoint.*

Sub-requirements

In the properties of a requirement, the **Sub-requirements** section enables you to define second-level requirements (or sub-requirements).

Milestones and Statuses

In the properties of a requirement, the **Milestones and Status** page enables to specify:

- **Expiration Date-Term of Adjustment:** this is the date limit by which the requirement must be fulfilled.
- **Creation date:** date on which the requirement was created.
- **Last Update:** this is the date on which the last import was made.
- **Official status (from import)**
 - To be validated
 - Validated
 - Updated
 - Deleted
 - *Regulations and requirements are never deleted automatically. If a regulation/requirement is obsolete, status passes to "Deleted".*
- **Internal status**

You can indicate if the requirement:

 - is **To be assessed**
 - has already been **Assessed**
 - N/A

MANAGING ACTION PLANS

- To use action plans within the framework of **HOPEX Internal Control**, see [Managing Issues and Action Plans](#).

All Action Plans

All action plans

Displays all action plans.

My action plans

Displays the action plans you own.

Delayed action plans

Displays the action plans where Planned End Date is overdue.

My delayed action plans

Displays the action plans you own and where Planned End Date is overdue.

Action Plan by Scope

Action plans managing Incidents

Displays action plans whose scope contains at least one incident.

For more details on managing incidents, see [Collecting Incidents](#) .

Action plans implementing controls

Displays action plans whose scope contains at least one control.

Action Plans remediating issues

Displays action plans whose scope contains at least one issue.

Action plans mitigating risks

Displays action plans whose scope contains at least one risk.



MANAGING KEY INDICATORS



Key indicators are metrics used by organizations to provide an early warning of increasing risk exposures in various areas of the enterprise.

They enable you to monitor indicator values (whether entered manually in **HOPEX** or through automated connectors). You can for example manage KPIs (Key Performance Indicators) or control indicators.

To administrate key indicators, see [Administrating Key Indicators](#)

- *Key indicators are available with **HOPEX Internal Control** and **HOPEX Enterprise Risk Management**.*

- 6 [Accessing Key Indicators](#)
- 6 [Defining Key Indicators](#)
- 6 [About Key Indicator Categories](#)
- 6 [More Key Indicator Characteristics](#)
- 6 [Consulting the Key Indicator Dashboard](#)
- 6 [Defining Measurement Frequency and Notifications](#)
- 6 [Viewing the Indicator Graph](#)
- 6 [Entering Periodic Key Indicator Values](#)

ACCESSING KEY INDICATORS

You can access indicator from:

- a list
- a tree displaying the different entities of your environment.

Accessing Key Indicators from a List

To access key indicators from a list:

1. in the IRM desktop, select **Libraries > Indicators > All Indicators**.
2. A list of all the indicators of your environment is displayed.

The following information is displayed in columns for each indicator:

- Current status
- Measurement freshness (days)
- Time to Failure
- Value
- Lower Threshold
- Higher Threshold

- *For more information on the provided information in columns, see [Defining Key Indicators](#).*

Accessing Key indicators by Entity

To access key indicators from a hierarchy of entities:

- > in the IRM desktop, select **Libraries > Indicators > By entity**.
Your organization's Entities hierarchy is displayed as a tree.

- *For each Entity, the sum of its immediate sub-Entities as well as the number of indicators for the entity are displayed.*

To connect indicators to a given entity:

1. Select **Libraries > Indicators > By entity**.
2. Right-click on the relevant Entity and select **Connect**.

DEFINING KEY INDICATORS

Creating a Key Indicator

To create a key indicator:

1. In the IRM desktop, select **Libraries > Indicators > All Indicators**.
2. Click **New**.
A creation window appears
3. Specify a **Lower Threshold** and a **Higher Threshold**.
4. Specify an Indicator **Category**.
The indicator category determines how the indicator values are interpreted and how the indicator status is computed:
 - **Standard**: the higher threshold represents the objective.
 - **Reverse**: opposite of standard
 - **Accepted Values**: All values within the defined thresholds are accepted
 - **Rejected Values**: all values within the defined thresholds are rejected.
 - For more information, see [About Key Indicator Categories](#).
 - If several algorithms are provided for an indicator category, the field **Key Indicator Interpretation logics** is proposed. You can select the desired algorithm to compute the indicator status. For more information, see [Relation between Indicator Category and Interpretation Logic](#).
5. Specify whether you need to aggregate values over a specific period of time.
The aggregation is not specified by default.
 - If you need to aggregate values, see [Specifying the Aggregation Period and Method](#).
6. Click **OK** to create your indicator.
 - You cannot change the KRI category, aggregation period and aggregation method after the KRI has been created.

Specifying the Aggregation Period and Method

Indicator values are not aggregated by default. You should explicitly state that the values need to be aggregated.

To aggregate values:

1. In the key indicator creation wizard, deselect the **Do not aggregate Key Indicator Values** check box.
Two additional fields appear in the wizard.

2. Specify the **Aggregation period**

) *An aggregation period is the period over which the indicator values are aggregated to compute the current indicator value and status.*

- Yearly
- Half-Yearly
- Quarterly
- Monthly
- Half-Monthly
- Weekly

3. Specify the **Aggregation method**

) *An aggregation method is the mathematical operation carried out over the indicator aggregated values in order to compute the indicator current value and status.*

- Sum
- Average

- *Note that new aggregation periods and aggregation methods can be created by your functional administrator.*
- *Once the key indicator has been created, it is no longer possible to specify another aggregation period or method.*

Example of a Key Indicator

) *Key indicators are metrics used by organizations to provide an early warning of increasing risk exposures in various areas of the enterprise.*

Below is an example of a Key indicator. It illustrates how key indicators are used as well as their characteristics.

A key indicator monitors the annual turnover of a legal entity. The objective is set to 12 million (€).

The KRI shall monitor the monthly turnover in order to ensure that the appropriate measures are taken if things do not go as expected.

It has been decided that the monthly turnover should always be between 900k and 1.1 million €. The KRI value is measured twice a month, which means the key indicator values entered each month are summed up to obtain the monthly turnover.

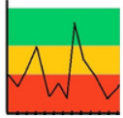
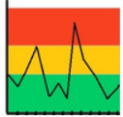
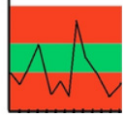
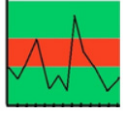
In this example the different characteristics described in **HOPEX** are as follows:

- **Lower Threshold:** 900k
- **Higher Threshold:** 1.1 million
- **Category:** Standard (all values above the higher threshold are considered to be good)
- **Aggregation period:** monthly
- **Aggregation** method: sum
- **Statuses** for the monthly turnover:
 - Operational - If higher than 1.1 million (higher threshold).
 - Warning – If between 800k and 900k
 - Unsatisfactory – If between 650k and 800k
 - Critical – If between 500k and 650k
 - Failed – If lower than 500k

ABOUT KEY INDICATOR CATEGORIES

) An indicator category specifies how the indicator values are interpreted and how Time to Failure is computed. It also specifies how the indicator status is computed through an associated interpretation logic.

Description of Key Indicator Categories

Key Indicator Category	Meaning	Visual representation
Standard	The higher threshold represents the objective. For values beyond the higher threshold, the key indicator is considered as "operational" (green color).	
Reverse	Opposite of "Standard" All values beyond the higher threshold are rejected. The lower the value the better it is.	
Accepted values	All values within the defined thresholds are accepted	
Rejected values	All values within the defined thresholds are rejected	

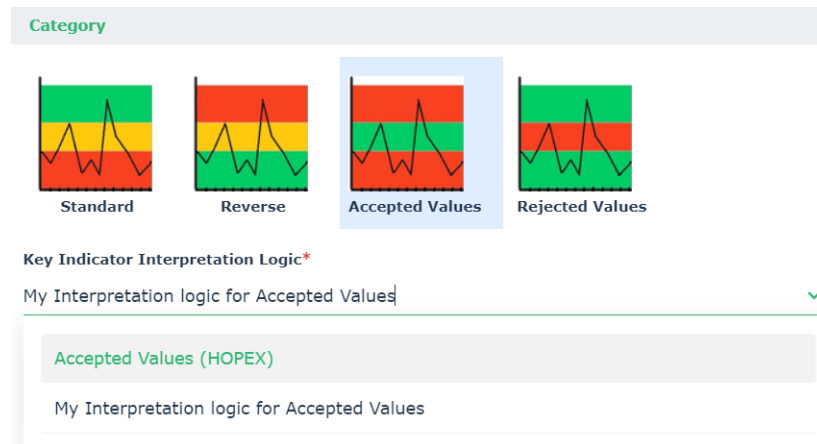
Relation between Indicator Category and Interpretation Logic

An indicator category is linked to an interpretation logic which uses an algorithm to compute the indicator status. Several interpretation logics can be associated to an

indicator category. It is therefore possible to have several ways of computing the status for an indicator category.

If several indicator interpretation logics are available for an indicator category, the interpretation logics are proposed at the time of indicator creation.

For example, if several interpretation logics exist for the Accepted Value category, then the following is displayed:



- *Key indicator interpretation logics can be created by your functional administrator.*

MORE KEY INDICATOR CHARACTERISTICS

After having created your indicator, you can modify some of his characteristics and describe it in a more detailed manner.

- *You cannot change the KRI category, aggregation period and aggregation method after the KRI has been created.*

Editing Key Indicator Parameters

Once the indicator has been created, you can no longer edit the indicator category, aggregation period or method. You can however edit a few parameters.

To edit parameters:

1. In the **Characteristics** indicator property page, expand the **Advanced** section.
2. Click **Edit Parameters**.

In the window that opens, you can edit:

- the **Lower Threshold** and **Higher Threshold**.
- the **Number of values used to compute Time to Failure**

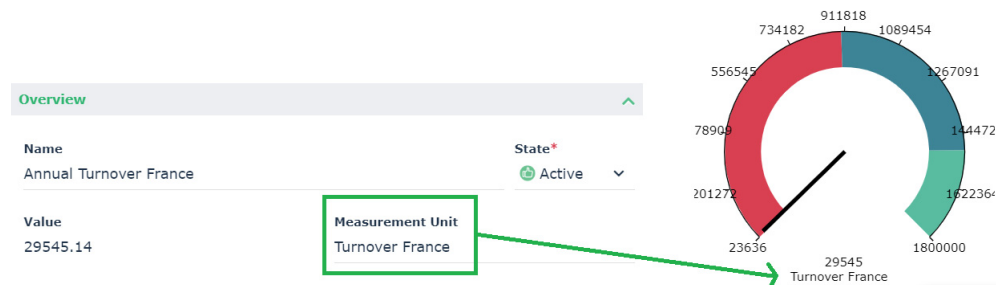
) *Time to Failure is the number of estimated days before the indicator turns to "Failed" status.*

- *The **Number of values used to compute time to failure** is the number of past values that should be taken into account. It is 12 by default. The higher the better but this could impact performance negatively. It is therefore important to find the right balance.*

Note that when you edit these parameters, Status and Time to Failure are automatically updated.

Defining a Measurement Unit to be Displayed in Reports

In the property page of a key indicator, the **Measurement Unit** field represents what the indicator is monitoring. The contents of the field is reused as a label for the Y axis in the indicator graphs.



For more information on graphs and reports, see [Viewing the Indicator Graph](#).

Activating / Deactivating a Key Indicator

A key indicator is activated by default when it is created. You may want to deactivate it if it reaches its end of life, if no more measurements are to be made. You can deactivate a key indicator by modifying its state.

To deactivate a key indicator:

1. Open the key indicator property page.
2. In the **State** field, select "Inactive".

If you set the state to "Inactive":

- The value and status of the key indicator is computed one last time
- It is no longer possible to enter new values
- All current notifications are deactivated
 - To be able to enter new values again and/or edit the properties of the key indicator, set the State to "Active".
 - The state of a key indicator should be distinguished from its status.

Specifying the Indicator Scope

To specify the scope of the indicator:

- > In the property page of the indicator, select the **Characteristics** page and expand the **Scope** section.

Here you can specify the associated:

- entities
 -) *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.*
- business processes
 -) *A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.*
- organizational processes
 -) *An organizational process describes how to implement all or part of the process required to make a product or handle a flow.*
- applications

To remove an indicator from a given entity:

1. In the property page of the indicator, expand the **Scope** section then select the **Entity** tab.
2. Remove the appropriate entity.

Specifying Action Plans

To define action plans on a key indicator:

1. In the properties of the key indicator, select the **Remediation** page.
2. Connect an existing action plan or create one as appropriate.
 -) *An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities.*
 - *For more information on action plans, see the corresponding information in the Common Features section of this Online help.*

CONSULTING THE KEY INDICATOR DASHBOARD

To consult your key indicator dashboard:

1. In the navigation menu, select **Library > Indicators**.
2. Open the property page of your indicator.

The dashboard gives you an overview of the computed characteristics of your indicator.

Annual Turnover France

Characteristics

Failed
Indicator Status

2 month(s)
Measurement Freshness

0 day(s)
Time to Failure

Overview

Name	State*
Annual Turnover France	Active

Value	Measurement Unit
29545.14	Turnover France

Indicator Status

Default statuses

The following statuses are available by default:

- Unknown
- Operational
- Warning
- Unsatisfactory
- Critical
- Failed

Their meaning depends on the indicator category and interpretation logics behind it.

- The indicator status is to be distinguished from the indicator state (which indicates whether the indicator is active or not).

The indicator status enables to issue a warning when necessary. For more information, see [Defining Measurement Frequency and Notifications](#).

Information about indicator status computation

The indicator status is computed based on:

- the indicator latest values
 - For more details on indicator values, see [Entering Periodic Key Indicator Values](#).
- the aggregation period
 -) An aggregation period is the period over which the indicator values are aggregated to compute the current indicator value and status.
- the aggregation method.
 -) An aggregation method is the mathematical operation carried out over the indicator aggregated values in order to compute the indicator current value and status.
 - For more details, see [Specifying the Aggregation Period and Method](#).

The status computation is triggered when:

- a new value is added
 - For more information, see [Entering Periodic Key Indicator Values](#).
- an existing value is deleted
- key indicator thresholds are edited
- the indicator state (active or inactive) has been modified
 - For more information, see [Activating / Deactivating a Key Indicator](#).

Time To Failure

Time to Failure is the number of estimated days before the indicator turns to "Failed" status.

A linear interpolation of past values is performed to compute Time To Failure.

You must specify the number of past values taken into account to compute Time to Failure. For more information, see [Consulting the Key Indicator Dashboard](#).

Value	Details
Unknown	Not enough data available (at least 2 aggregated values should be available)
Unforeseen	The indicator values evolve in a way which makes it impossible to reach/predict the Failed status. <ul style="list-style-type: none">- 9999 is displayed in the Time to Failure column of the list of indicators.
0 day(s)	The indicator status is "Failed" already.

Indicator Freshness

Indicator freshness is the time elapsed (number of days) since the last indicator value entered.

It is rounded to the closest integer.

Indicator Value

In the property page of the indicator, you can also find the Value of the indicator.

The indicator value consists of the last aggregated measurement of the indicator.

- *If no aggregation period or method have been defined, it consists of the last measurement of the indicator.*

See also: [Entering Periodic Key Indicator Values](#).

DEFINING MEASUREMENT FREQUENCY AND NOTIFICATIONS

Specifying Measurement Frequency

To specify the measurement frequency of an indicator:

1. See [Accessing Key Indicators](#).
2. In the properties of an indicator select the **Values** page.
3. In the **Measurement frequency** section, select a steering calendar:
 - **Daily** Measurement Frequency
 - **Monthly** Measurement Frequency
 - **Weekly** Measurement Frequency

This steering calendar is used to send notifications to appropriate users.

Managing User Notifications

HOPEX IRM enables you to send automatic notifications based on the key indicator status and the date of its last measurement. This way, you can ensure that the indicator owners properly manage indicators.

To specify or modify user notifications:

- › In the property pages of a key indicator, select the **Notifications** page.

You can choose to send periodic notifications:

- to a specific person
 - *By default, the owner of a key indicator receives notifications. Here you can specify another person.*
 - *The notifications sent to appropriate users prompts them to enter values for the key indicator they are in charge of monitoring. For more information, see [Entering Periodic Key Indicator Values](#).*
 - to a set of users (when the indicator reaches a specified status or when the last measurement is older than a specified number of days).
-

Entering Periodic Key Indicator Values

HOPEX IRM enables the indicator owner or other authorized persons to manually enter a key indicator value in order to feed the key indicator.

To enter a key indicator value:

1. In the properties of an indicator, select the **Values** page.
2. Click **New** and enter a value.
3. Modify the default date if necessary.

4. Click **OK**.

- *Notifications can be set up so that you are periodically reminded of the need of entering periodic values. For more details, see [Managing User Notifications](#).*

The values entered periodically enable to produce the value which is indicated in the key indicator **Characteristics** page.

VIEWING THE INDICATOR GRAPH

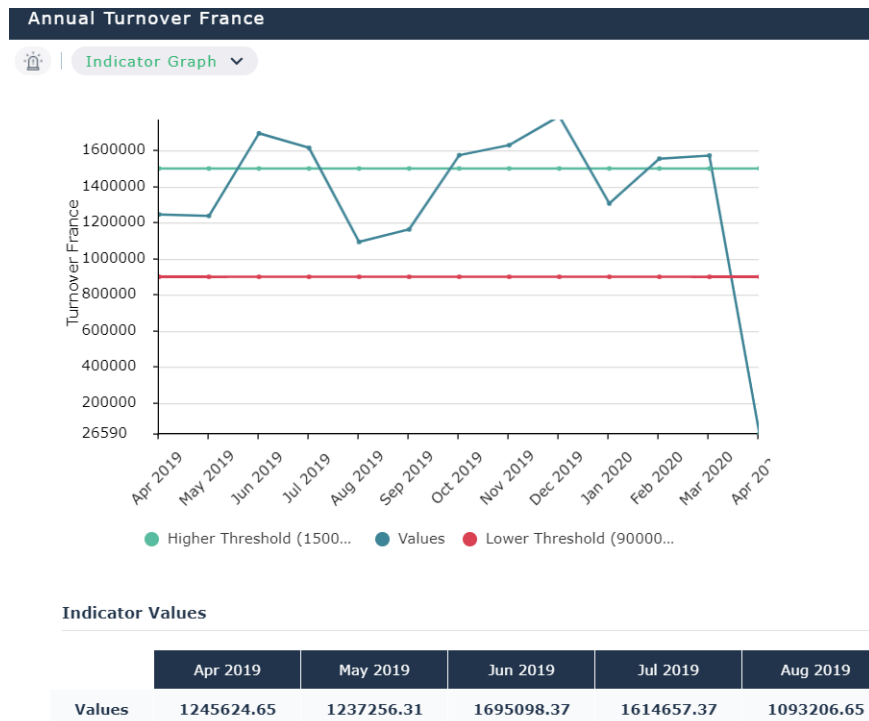
HOPEX IRM enables you to display an indicator graph for a specific indicator.

To access this graph:

- > In the property page of your indicator, select the **Indicator Graph** page.

The values of the indicator are displayed in a table below the graph.

- To display a label on the Y axis of the graph, see [Defining a Measurement Unit to be Displayed in Reports](#).



HOPEX IRM also offers to view reports which enable to compare various indicators. See [Key Indicator Reports](#).

MANAGING ASSESSMENT CAMPAIGNS



The IRM solutions (Integrated Risk Management) allow you to assess controls and risks through assessment campaigns.

- 6 [Introduction to Assessment by Campaign](#)
- 6 [Accessing Assessments by Profiles](#)
- 6 [Accessing Assessment Templates](#)
- 6 [Preparing the Assessment Work Environment](#)
- 6 [Risk and Control Campaign Assessment](#)
 - *You can also directly assess risks and controls, without using questionnaires. See "Direct Assessment" in **HOPEX Enterprise Risk Management** and **HOPEX Internal Control** documentation.*
 - *For more details on assessment reports, see [Assessment Follow-Up Reports](#).*

INTRODUCTION TO ASSESSMENT BY CAMPAIGN

The **HOPEX IRM** Desktop enables assessments on your risks or controls 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.

What is assessment?

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 sessions and campaigns

An assessment is based on concepts:

- assessment sessions
 -) *An assessment session is an assessment carried out over a determined time period. When an assessment session is published, an assessment form containing questions is sent to targeted users.*
- assessment campaigns
 -) *An assessment campaign enables creation and planning of several assessment sessions over a given time period.*

An assessment session is defined by its **scope** and a **questionnaire template**.

-) *The scope of an assessment session is defined by the objects to be assessed, the context of the assessment, and the list of respondents.*

Questionnaire templates and questionnaires

Assessment **questionnaires** are sent to appropriate **respondents** .

-) *An assessment questionnaire is a list of questions relating to a particular object and addressed to users.*
-) *A respondent is a person in the enterprise questioned in the context of the assessment. This person should complete the assessment questionnaire and return it.*

Questionnaires of an assessment session are described in a **questionnaire template** defined:

- directly in the assessment session:
- in an **assessment template**.
 -) *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 assessment template can also supply deployment queries activated from one session to another to better determine the scope of objects to be assessed, the context and even the respondents.*

Quotation rules

Assessment session unitary results are then calculated from respondent answers according to **Quotation Rules** defined for the session.

) *A quotation rule defines the list of answers used to calculate the value of an assessment characteristic. It also provides the plugIn handling the calculation.*

Aggregation schemas

Assessment results are then consolidated according to one or several **aggregation schemas**.

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

ACCESSING ASSESSMENTS BY PROFILES

You can access the functions of assessment campaigns from various profiles and desktops:

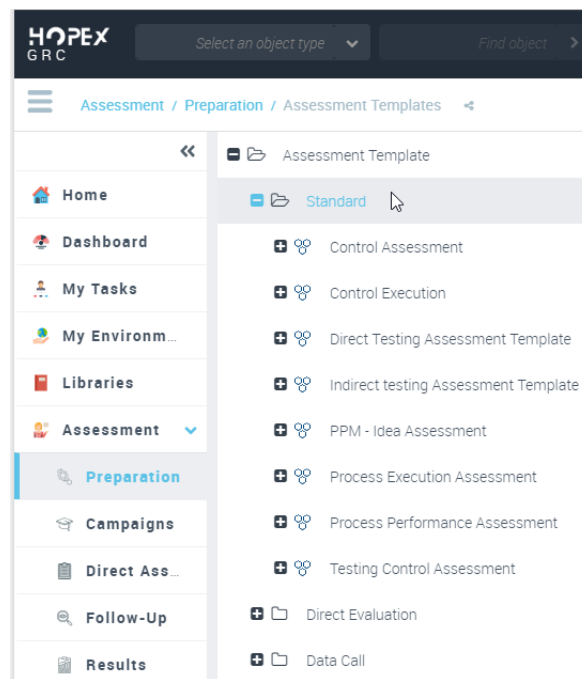
Profile	Action	Desktop
IRM functional administrator	<ul style="list-style-type: none">- Assign roles to persons of the enterprise- Define the organization (entities, processes,...)- Determine respondents (risk assessors for each entity)	HOPEX IRM desktop
IRM manager (Internal Controller)	<ul style="list-style-type: none">- Create assessment campaigns- Create assessment sessions- Follow up assessment sessions	HOPEX IRM Desktop
IRM Contributor (Lite)	<ul style="list-style-type: none">- Accept or refuse questionnairesReply to questionnaires	IRM Contributor desktop

ACCESSING ASSESSMENT TEMPLATES

- 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 assessment template can also supply deployment queries activated from one session to another to better determine the scope of objects to be assessed, the context and even the respondents.
- For more details on assessment template customization, see **HOPEX Power Studio - Assessments: [Assessment Templates](#)**.

To access assessment templates:

- > In the navigation pane, click **Assessment > Preparation > Assessment templates**.
Assessment templates appear.



The assessment templates use:

- 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: Criticality.
- a 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. The questionnaire template is defined either

*at assessment template level or assessment session level.
Questionnaires sent to respondents are generated from the definition
supplied in the questionnaire template.*

From the navigation menu **Assessment > Preparation** you can also access assessed characteristics and questionnaire templates.

PREPARING THE ASSESSMENT WORK ENVIRONMENT

Pre-requisites to control assessment

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

- connected controls to processes
- connected processes to organization entities
 - See [Contextualizing Controls](#).
- defined respondents, and specified for each one the entity to which he/she is attached as well as an email.
 - See [Specifying control responsible users](#).

Prerequisites to risk assessment

Before starting a risk assessment campaign, check that you have:

- connected risks to at least one entity
 - See [Risk characteristics](#).
- specified a respondent in the **Risk Assessor** field of the entity properties.
 -) *The risk assessor is in charge of assessing risks within the framework of assessment campaigns.*
 - See [Specifying risk assessor](#).

RISK AND CONTROL CAMPAIGN ASSESSMENT

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.

The assessment can also be done directly on the objects, outside the assessment campaign.

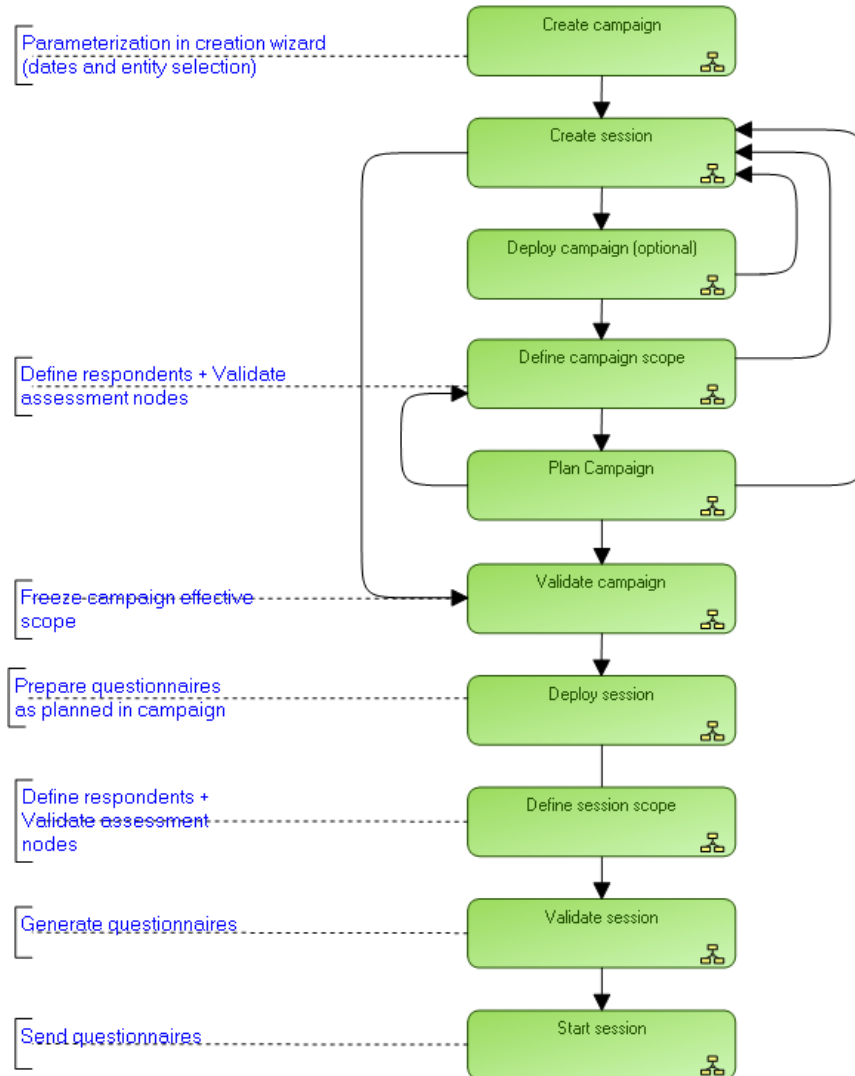
- For more details on the assessment mechanism, see [Introduction to Assessment by Campaign](#).

Questionnaires are sent via an assessment session, which corresponds to an assessment over a specified period of time.

Before creating a session, you must prepare the work environment and then create a campaign, which includes a set of assessment sessions.

Assessment Campaign Workflow Steps

Find below the assessment campaign workflow.



Standard Assessment Workflow

Creating an Assessment Campaign (with model)

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. See [Session creation mode](#).

To create a control or risk assessment campaign with the templates provided as standard:

1. In the navigation menu, click **Assessment > Campaigns**.
The list of campaigns appears in the edit area.
2. Click **New**.
The campaign creation page appears.
3. Enter the name of the campaign.
4. Select the **Assessment Template**.
 - See [Accessing Assessment Templates](#).
5. Modify the **Calendar** if required.
 - *The calendar serves to initialize begin and end dates of the assessment campaign.*
6. Specify the **Begin Date** and the **End Date**.
7. Click **Next**.

8. In the **Scope Selection** window, select the objects that define the assessment context.
The tree allows you to select controls or risks assessed **in their context**.
A control or risk is assessed in the context of the elements of the branch that extends from the object in question up to the root.

Multiple Assessment - Select Assessed Objects + -

The context(s) corresponding to your previous selection are presented below in a hierarchy. You can expand the hierarchy and select either a whole set of contexts or a single context. All objects applying to these selected contexts will be included into your multiple assessment table unless you deselect them.

Risks per Business Process :

☒ Select parents and sub-elements | ☒ Expand the selected items

+ ☐ SOX - Taxes

- ☒ Support Process

☐ ⚠ Contractual risk

☐ ⚠ Deontological risks

☐ ⚠ Legal & Regulatory risks

☐ ⚠ Risks of Image

☐ ⚠ Taxes sanction

- ☒ Accounting

☒ Manage HR Administration and Payroll

☐ Develop and Manage Human Capital

In the above example, if you selected the "Accounting" process, 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.

9. Click **Next**.

10. 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 or controls)
- context objects (entities, processes, etc.)
- assessment nodes which correspond to objects placed in their context objects, associated with respondents.
- respondents

11. Click **OK**.

Next step: [Creating an Assessment Session](#).

Creating an Assessment Session

Previous step: [Creating an Assessment Campaign \(with model\)](#)

Session creation mode

To create an assessment session:

1. Open the properties of the campaign and select the **Sessions** page.
2. In the **Assessment Sessions** section, click **New**.
The session creation wizard opens.

Within the context of a campaign with a template, the session characteristics are automatically inherited from the template defined on the assessment campaign.

When you have not defined a template on the campaign, you can define the session in one of the following modes:

- **From an Existing Template:** assessment is created from an existing assessment template. All information characterizing the session is described in the template.
- **In Ad-Hoc mode:** the assessment is created simply from lists to be completed so as to specify the scope objects.
- **In Expert mode:** this mode is reserved for experts who want to define queries and macros. Assessment is carried out from deployment collections constituting a first step to reuse of object lists defining a scope.

From a campaign with template

To create a session as part of a campaign with a template:

1. In the session creation wizard, enter the session name.
2. Specify when to start the evaluation session. See [Session start options](#).
3. Click **OK**.

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](#).*

From an existing template

Within the context of a campaign without predefined template, you can apply a template to the session:

1. In the session creation wizard select the **From an Existing Template** option and select the assessment template you want to use.
2. Specify assessment session dates:
 - **Assessment Planned Begin Date** is fixed at today's date
 - **Assessment Planned End Date.**
3. Click **Next.**
4. Select the **Perimeter** that corresponds to the object from which the object list to be assessed will be established.
5. Click **Next.**
A preview report of the scope calculated for the session is presented for information.
6. Click **Next.**
7. Specify when to start the session. See [Session start options](#).
8. Click **OK.**

In Ad-hoc mode

Ad-Hoc assessment session creation mode allows you to explicitly define objects characterizing the scope of your session.

To create an assessment session in Ad-Hoc mode:

1. In the session creation wizard, select the **Ad-hoc** mode:
2. Click **Next.**
3. Complete each of the sections with the objects that interest you:
 - **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: Criticality.*
 - **Assessed Objects**

The Connect button allows you to select objects by filtering these by assessable object type.
 - (Optional) **Context Objects**

) *A context object is an object in the framework of which the assessment is carried out. For example, a risk can be assessed in the framework of an entity, a control can be assessed in the framework of a process).*
 - **Assessors:** you may select a **Respondent** as well as **Person Assignments**.

) *A respondent is a person in the enterprise questioned in the context of the assessment. This person should complete the assessment questionnaire and return it.*

- *Person assignment enables specification of the profile to which you wish to address the questionnaire when the same person has several profiles.*
4. Click **Next.**
5. Create a **Questionnaire Template**.
 - *You cannot connect existing questionnaire templates.*

6. In the dialog boxes that follow, you can specify the **Quotation Rule** to be applied.
 -) *A quotation rule defines the list of answers used to calculate the value of an assessment characteristic. It also provides the plugIn handling the calculation.*
 - *For more details, see [Quotation Rules](#).*
7. Click **OK**.

In Expert mode

Expert creation mode is reserved for experts who want to use queries or macros to define scope of their assessment session.

To create an assessment session in **Expert** mode:

1. In the session creation wizard, select the **Expert** mode.
2. In the **Assessment Scope Definition** field, specify how you wish to define scope:
 - "By Tree"
 - "By Collection"
 - *For more details on assessment scope definition, see [Defining Assessment Template Properties](#).*
3. Click **Next**.
4. Complete the list of assessed characteristics explicitly.
 - *For more details, see [Managing Assessed Characteristics](#).*
5. Complete assessment scope using deployment collections to determine:
 - the list of objects to be assessed
 - the list of objects defining the assessment context
 - the list of respondents
 - *For more details, see [Creating Assessment Deployment Collections](#).*
6. Click **Next**.
7. Create a **Questionnaire Template**.
8. Click **Next**.
9. Specify the **Quotation Rules** to be applied as well as a MetaTest if required.
 -) *A quotation rule defines the list of answers used to calculate the value of an assessment characteristic. It also provides the plugIn handling the calculation.*
 - *For more details, see [Quotation Rules](#).*
10. Click **OK**.
11. In the session creation wizard, click **Next**.

A preview report of the scope calculated for the session is presented for information.
12. Click **Next**.
13. Specify when to start the session. See [Session start options](#).
14. Click **OK**.

Session start options

You have several possibilities to start a session:

- **Not now**
- **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](#)
 - validate: [Validating Assessment Sessions](#)
 - start: [Starting Assessment Sessions](#)
- **As soon as possible**: after saving, in batch mode
- **Schedule**: later, specifying the date and hour in UTC format

Next step: [Deploying Assessment Campaigns](#).

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.

To deploy a campaign, you must have created a campaign with a template.

– *This step is optional. If you are not deploying the assessment campaign, go directly to [Validating Assessment Campaigns](#)*

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 predefined date and time*
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 if necessary (entities and processes)*

Next step: [Defining assessment campaign scope](#).

Defining assessment campaign scope

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](#)

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**.

Next step: [Planning Assessment Campaigns](#).

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 the objects (for example risks) in their context (for example entities).
 - If you don't see the previously created assessment sessions, click the **Refresh** button.

Assessment Campaign-4				
<div> Planning ▼ </div> <div>Refresh</div>				
<input type="checkbox"/>	BP Context	Assessed Object	Respondent	E-mail
<input type="checkbox"/>	Long Term Investment, Procurement, Support...	⚠ Bad Definition of Agency...		
<input type="checkbox"/>	Financial Reporting, Financial Cycles, Support...	⚠ Bad Image Impact	Adam	webeval@...
<input type="checkbox"/>	Financial Reporting, Financial Cycles, Support...	⚠ Bad Technology Choices	Edouard	webeval@...
<input type="checkbox"/>	Domestic taxes, Support Process	⚠ Budget overrun	Edouard	webeval@...
<input type="checkbox"/>	Support Process	⚠ Contractual risk		
<input type="checkbox"/>	Domestic taxes, Support Process	⚠ Data Retention and Dispo...		

- Respondents are specified at step [Defining assessment campaign scope](#).

Next step: [Validating Assessment Campaigns](#).

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.

Next step: [Deploying 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 if necessary (entities and processes)*

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 **Session** tab.
2. In **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.

Next step: [Defining assessment session scope](#).

Defining assessment session scope

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 [Defining assessment campaign scope](#).*

Defining assessment session scope

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**.

Next step: [Validating Assessment Sessions](#).

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 **Session** tab.
2. In the **Assessment Session** section, click the session that interests you, then **Assessment Session > 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. 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.

*To configure these, see [Assessment Templates](#) in the **HOPEX Power Studio** - Assessment documentation.*

*In the solution, questionnaire templates are available in the pane concerning campaign management > **Preparation > Questionnaire Templates**.*

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**.

Next step: [Starting Assessment Sessions](#).

Starting Assessment Sessions

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

To send questionnaires to respondents:

1. Select **Assessment Campaigns > Campaigns**.
The list of campaigns appears in the edit area.

2. Select the campaign that interests you and click **Properties**.
3. In the **Sessions** section, click the session that interests you, then **Assessment Session > 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.
) An assessment questionnaire is a list of questions relating to a particular object and addressed to users.

Completing Questionnaires

The steps described here concern questionnaire respondents.

Accessing Assessment Questionnaires

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

To complete questionnaires:

1. In the navigation menu, click **My Tasks > Assessment > Questionnaires to answer**.
The list of questionnaires to be completed appears.
2. Select the questionnaire that interests you and click **Display Questionnaire**.
3. Select the questions 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 by mistake, you can ask the session manager to transfer the questionnaire to another person.

To make a transfer request:

1. In the navigation menu, click **My Tasks > Assessment > Questionnaires to answer**.
2. Click the icon of a questionnaire and select **Assessment Questionnaire (To Be Completed) > Transfer Request**.

The questionnaire switches to the "To Reassign" status.

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:

- > Open the properties of the assessment session and select the **Reports > Follow-Up** tab.
 - For more details on this report, see [Campaign results tree](#).

Validating Assessment Questionnaires

To access the list of assessment questionnaires completed by respondents:

1. In the navigation menu, click **My Tasks > Assessment > Questionnaires to review**.
In the page that appears, a section concerns the questionnaires to be validated.
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. In the navigation menu, click **My Tasks > Assessment > Questionnaires to review**.
In the page that appears, a section concerns the questionnaires to be validated.
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](#).

Viewing assessment campaign reports

Reports specific to assessment campaigns are available. For more details, see [Assessment Follow-Up Reports](#).

Reassigning questionnaires

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

To reassign a questionnaire:

1. In the navigation menu, click **My Tasks > Assessment > Questionnaires to review**.
In the page that appears, a section concerns the questionnaires to be reassigned.
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.

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 **Session** tab.
2. In the **Assessment 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.*

Consulting Assessment Results

The results of the control and risk assessment can be presented in dedicated reports that facilitate the analysis of the assessed objects. For more details, see [IRM Reports](#).









IRM REPORTS



Several reports deal with global IRM-related issues (Integrated Risk Management).

- [Key Indicator Reports](#)
- [Action Plan Follow-up Reports](#)
- [Assessment Follow-Up Reports](#)
- [Regulatory Compliance Reports](#)

For more information on solution-specific reports, see the corresponding documentation.

- [Report Related to Risks](#)
- [Reports Related to Controls](#)
- [Reports Related to Incidents](#)
 - See also the summary table about report availability: [IRM Report Availability](#)

IRM REPORT AVAILABILITY

Available reports depend on the profile and the solution used.

Profiles/Topics	Risks	Controls	Indicators	Compliance	Incident	Action plans
GRC manager	X	X	X	X	X	X
Risk Manager	X		X			X
Internal Control Director		X	X	X		X
Risk Manager Incident and Loss Administrator	X			X	X	X

KEY INDICATOR REPORTS

- For more information on key indicators, see [Managing Key Indicators](#)

HOPEX IRM offers several reports to compare indicators.

To access reports on indicators:

- > In the navigation menu, select **Analysis > Indicators**.

The following reports are available:

- Indicator comparator
- Multi-indicator graph
- Multi-indicator graph (gauges)

- **HOPEX IRM** enables you to display a graph specific to an indicator. For more information, see [Viewing the Indicator Graph](#).

Indicator Comparator

This report enables you to compare two indicators on the same line graph.

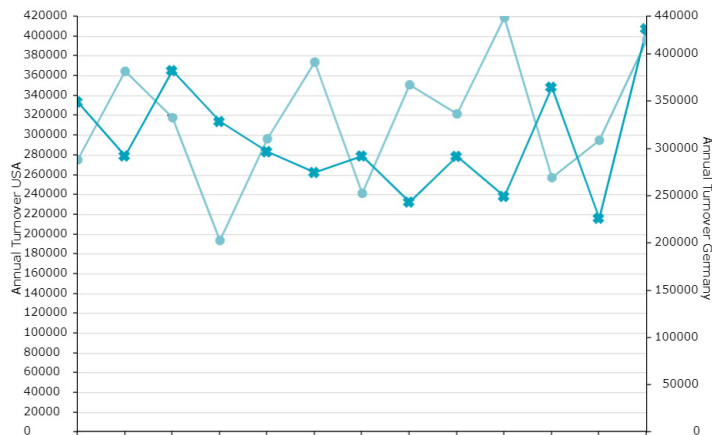
Access path

Analysis > Indicators > Indicator comparator

Parameters

Parameters	Remarks
Primary Key Indicator	Mandatory
Secondary Key Indicator	Mandatory
Aggregation Period	Mandatory
Aggregation Method	Mandatory

Results



Multi-Indicator Graph (Gauges)

This report enables you to display several key indicators through the display of several gauges.

Access path

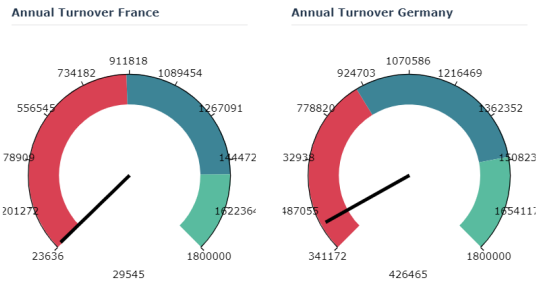
Analysis > Indicators > Multi-indicator graphs

Parameters

Parameters	Remarks
Number of columns	Mandatory - You can choose the number of columns best suited to display your indicators.
Key Indicators	Mandatory

Results

France vs Germany



Multi-Indicator Graph

This report enables you to display several key indicators on several line graphs.

Access path

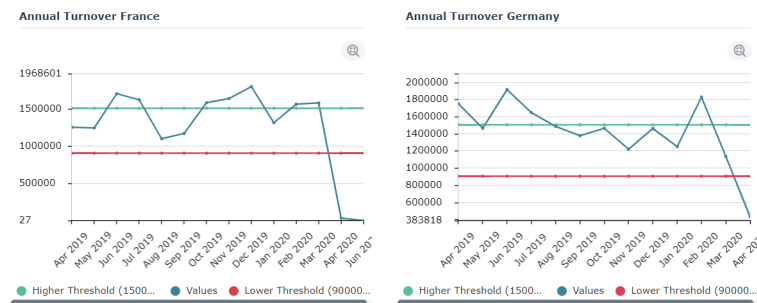
Analysis > Indicators > Multi-Indicator Graphs

Parameters

Parameters	Remarks
Number of columns	Mandatory
Key Indicators	Mandatory

Results

France vs. Germany





ACTION PLAN FOLLOW-UP REPORTS

- For more information on action plans, see [Managing Action Plans](#).

Action Plan Follow-Up

To follow up action plans:

- > Select **Analysis > Action Plans > Follow-Up** Follow-Up.

Access path

Analysis > Action Plans > Follow-Up

Result

This report enables the session manager to view whether questionnaires were completed between the planned start dates and the end of the assessment session.

The report is presented as a bar chart: It comprises several graphs:

- bar charts
- pie charts

The action plans are represented in their different contexts (processes and entities).

Action plans by status

This bar chart presents action plan statuses.

Action plans by progress

This pie chart presents action plan breakdown according to their status. Possible statuses are the following:

- On Time
 - in progress
 - with due date exceeding 30 days
- Delayed:
 - in progress
 - with due date earlier than current date
- Approaching due date:
 - in progress
 - with due date between 0 and 30 days inclusive
- Canceled
- Closed

Action plan by priority

This pie chart presents action plan breakdown according to their priority.

Possible priorities are the following:

- Critical
- High
- Medium
- Low

Action plans by category

This pie chart presents action plan breakdown according to their category.

Possible categories are as follows:

- Corrective
- Preventive

Action plans by entity

This bar chart presents breakdown of action plans for each entity.

- x-axis: all entities
- y-axis: number of action plans linked to each entity and sub-entity
 - *If no entity is selected, all root entities are taken by default.*

Action plans by process

This bar chart presents breakdown of action plans for each process.

- x-axis: all processes (business and organizational)
- y-axis: number of action plans linked to each process and sub-process
 - *If no process is selected, all root processes are taken by default.*

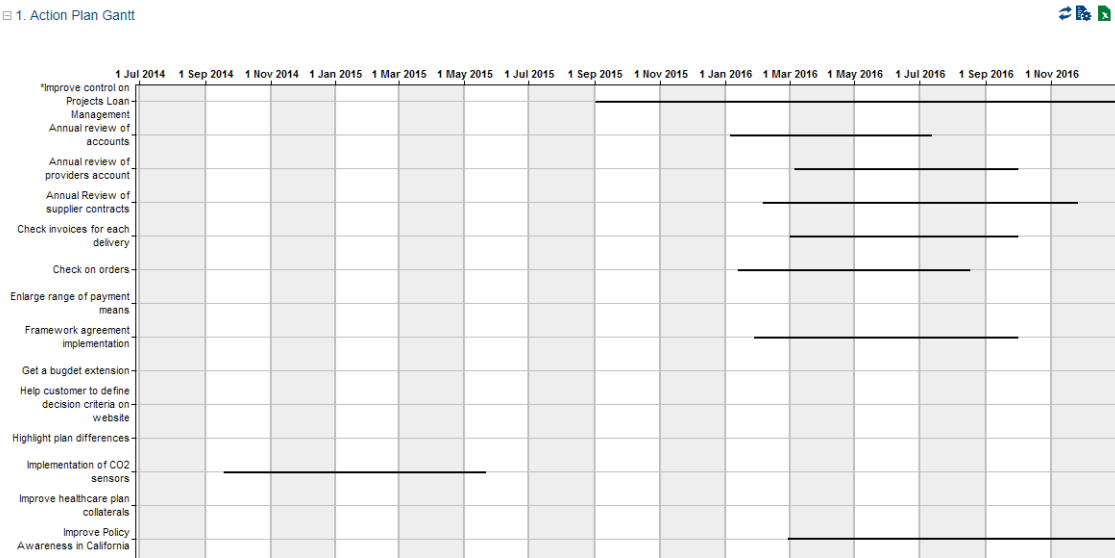
Gantt report

This report displays all action plans in the form of a Gantt chart.

To generate a Gantt chart of action plans:

1. Select **Analysis > Action Plans > Gantt**.
2. Click **New** then **Next**.
3. Click **Connect** to select action plans.

4. Click **OK**.
The Gantt of action plans appears.



ASSESSMENT FOLLOW-UP REPORTS

To access IRM assessment reports:

- > In the navigation pane, click **Assessment > Results**.

Assessment

Campaign results tree

This report presents results of a given execution campaign session. It presents entities/processes/controls as trees and indicates for each assessed control whether it is satisfactory or not.

Access path

Assessment > Results > Control Assessment Campaigns > Campaign Results Tree.

Parameters

Parameters
Campaign
Assessment session

Campaign Result Matrix by Entity

This report presents as a matrix the results of each session of a given assessment campaign.

Access path

Assessment > Results > Control Assessment Campaigns > Campaign Result Matrix by Entity.

Parameters

Parameters
Campaign
Entity
Entity type

Aggregation Report

The aggregation report presents in tree form all objects from the selected root entity, together with their last assessment.

Access path

Assessment > Results > Aggregation

Parameters

Parameters	Remarks
Begin Date	
End date	By default current date
Context root	Tree root entity
Aggregation schema	An aggregation schema should be selected from the proposed list
Assessed characteristics	Assessed characteristics proposed depend on the selected aggregation schema.

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

Follow-Up

Session Follow-Up

This report enables assessment session follow-up.

Access path

Reports > Execution > Execution Session Follow-Up

Parameters

Parameters
Session

Result

A summary displays general information on the current assessment session.

This report presents a number of charts concerning assessment progress:

- Percentage of completed questionnaires
- Distribution of questionnaires by status
- Distribution of questionnaires delegated/not delegated
- Distribution of questionnaires by status, for each respondent
- Distribution of questionnaires by status, for each assessed object

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%
Damage 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.

REGULATORY COMPLIANCE REPORTS

Requirement Location Matrix

This report enables simple location of requirements.

Access path

Reports > Regulatory compliance > Requirement Location Matrix

Parameters

Parameters	Parameter type	Comment
Begin Date	Date	Optional All requirements created after this date are selected.
End date	Date	Optional All requirements created after this date are selected.
Parent context	The context object can be a(n): <ul style="list-style-type: none">- Organizational process- Business process- Entity- Regulation	Mandatory Parent of context elements displayed in the matrix
Localized requirements	List of requirements possibly filtered by: <ul style="list-style-type: none">- Requirement- Entity- Regulation	Mandatory Requirements to be displayed in the matrix

Result

The requirement location matrix displays links between:

- a list of requirements
- sub-elements of a root context object
 - *The report is empty if the selected context object has no sub-objects*

Requirement Identification

This report consists of several graphs and gives an overview of the requirements recently created as well as their status.

This report presents distribution of requirements according to several perspectives:

- entities
- processes

Access path

Reports > Regulatory compliance > Requirement Identification

Parameters

Parameters	Remarks
Begin Date	Optional All requirements created after this date are selected.
End date	Mandatory Initialized with current date All requirements created after this date are selected.
Context object	Optional The context object can be: - an entity - a process

You can specify context objects enabling display of requirements linked to:

- Entities
- Processes

To connect context objects:

1. In the appropriate frame, click **Connect**
2. In the window that appears, select the objects to connect through a tree.

Results

To obtain the list of requirements making up a bar chart bar:

- > Click the bar chart bar that interests you.
The list of requirements taken into account is presented at the bottom of the edit area.



IRM SOLUTION WORKFLOWS

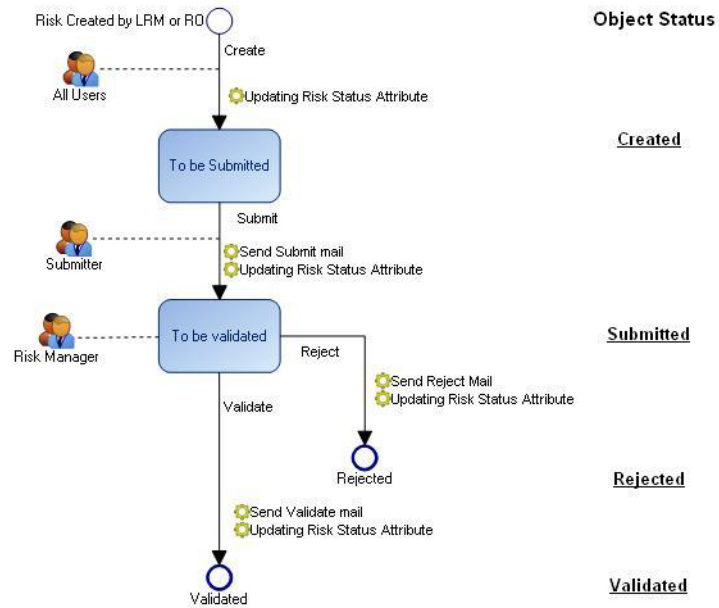


IRM (Integration Risk Management) activities are performed via ready-to-use workflows.

Workflow transitions are available in the pop-up menus of objects to which the workflow relates.

- 6 [Risk Workflows](#)
- 6 [Testing Workflows](#)
- 6 [Assessment Workflows](#)
- 6 [Action Plan Workflows](#)
- 6 [Incident Workflow](#)

RISK WORKFLOWS

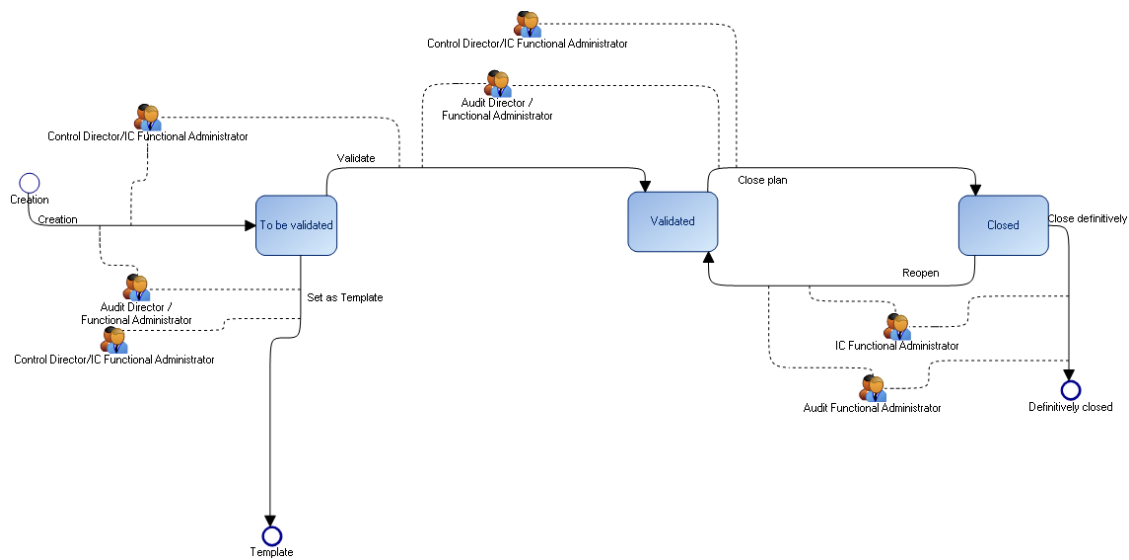


- For more details on the characteristics of risks and risk-related workflow, see [Managing Risks](#).

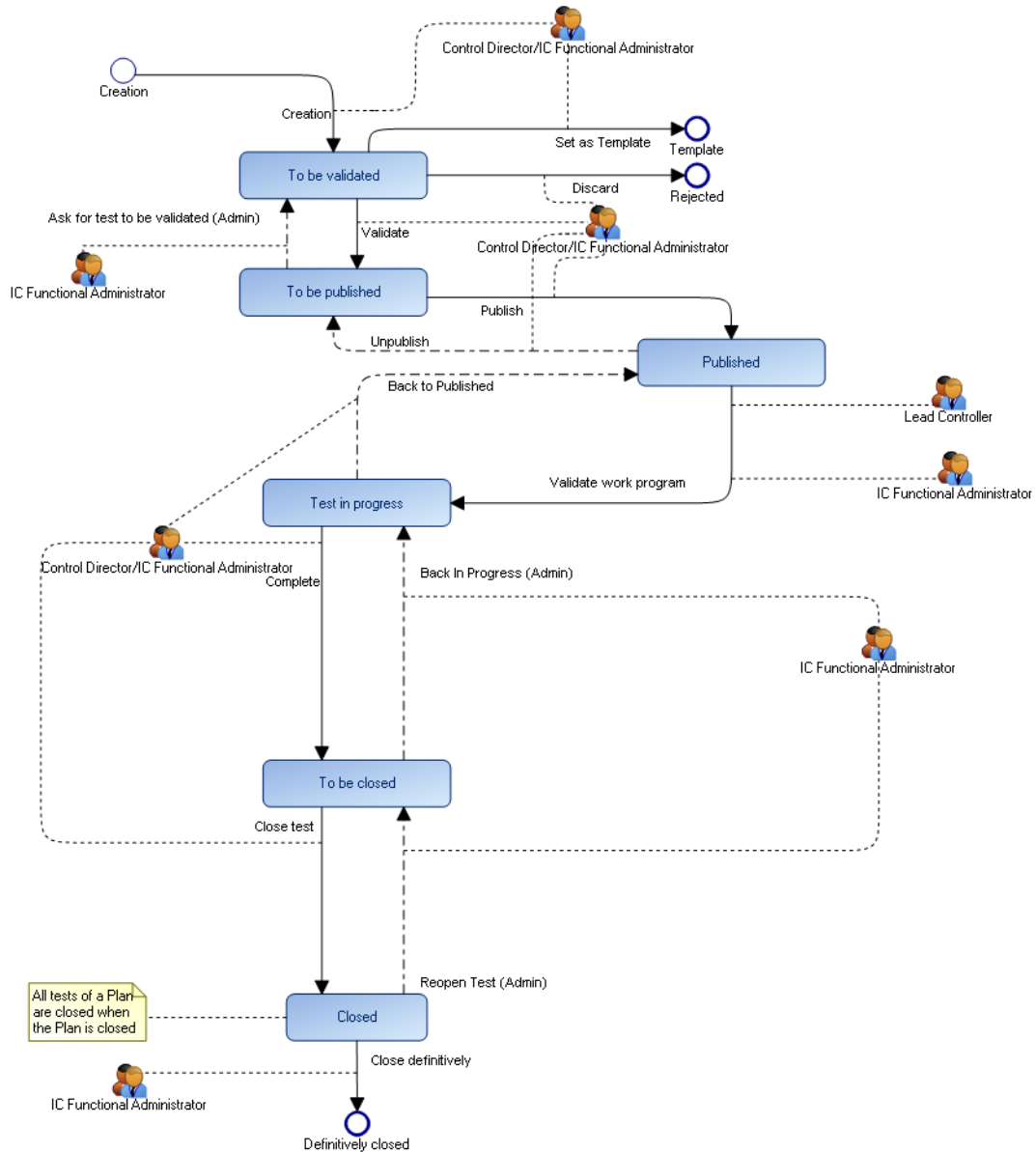
TESTING WORKFLOWS

- For more details on testing, see [Control Testing](#).

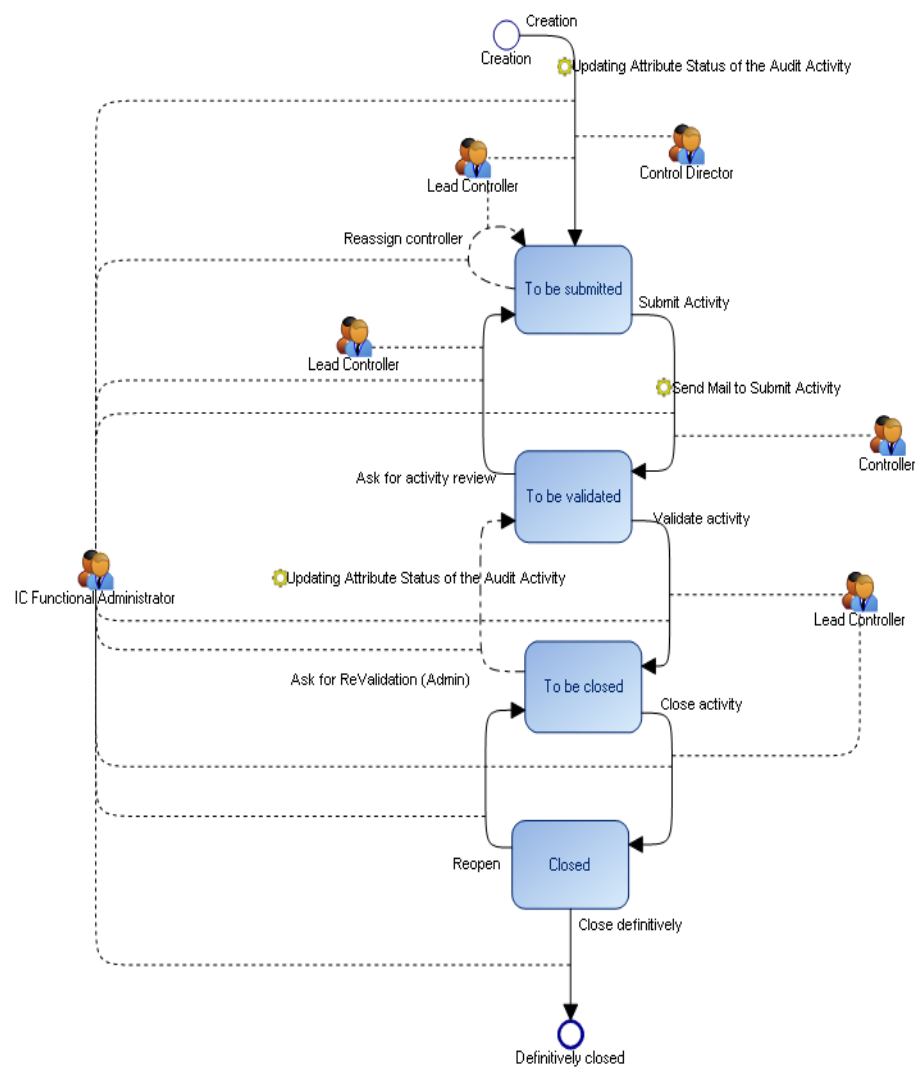
Test Plan/Audit Plan Workflow



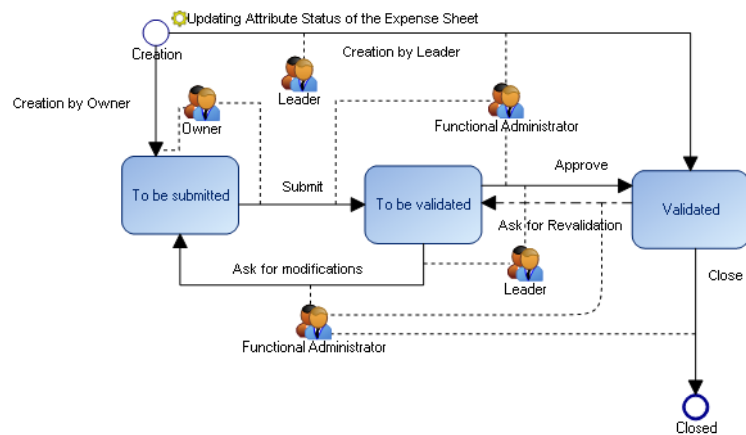
Test Workflow



Test Activity Workflow



Expense Sheet Workflow

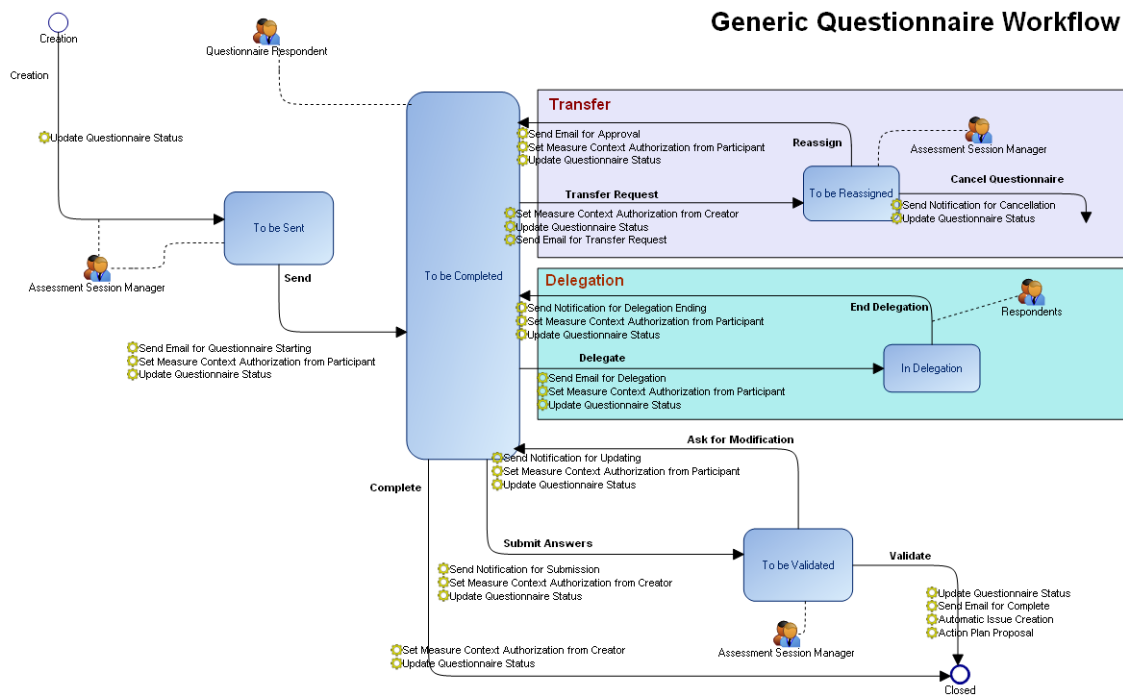


ASSESSMENT WORKFLOWS

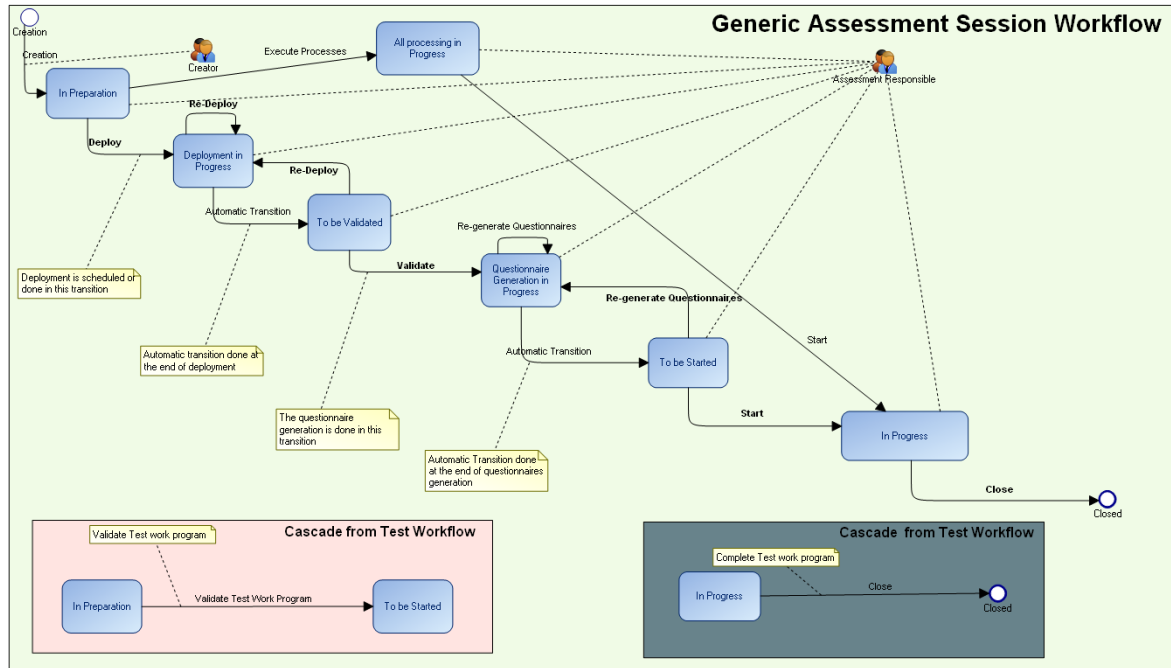
For more details on the workflow:

- Of control assessment campaigns, see [Generic Assessment Workflows](#).
 - Of control execution, see [Automatic Assessment Workflows](#).
- These workflows are detailed in the **HOPEX Power Supervisor - Assessment guide**.

Questionnaire Workflow



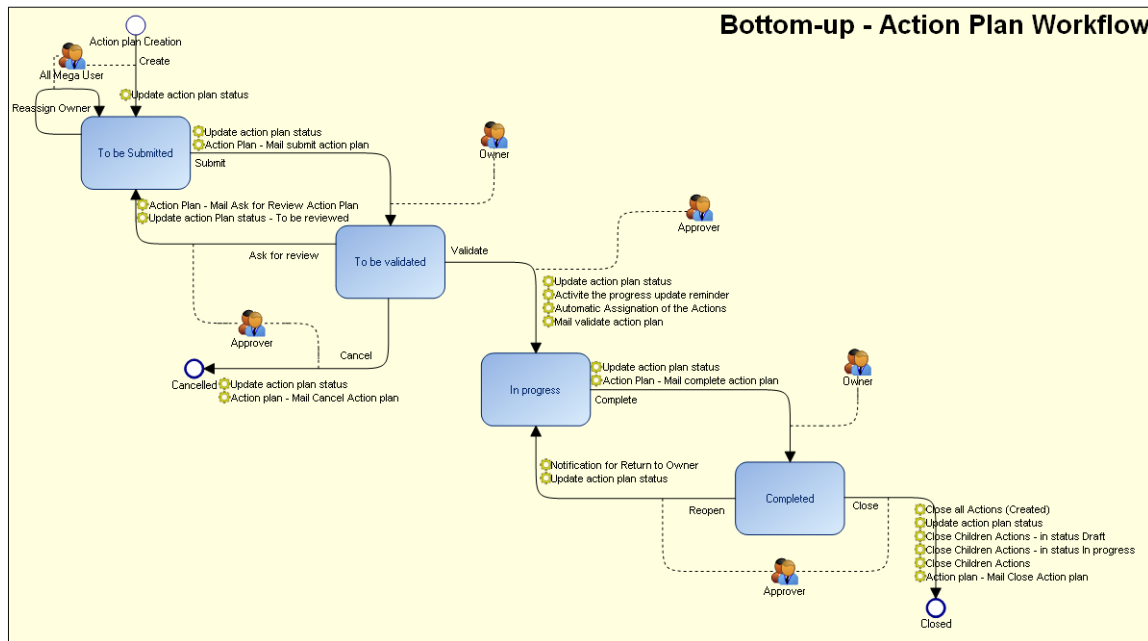
Assessment Session Workflow



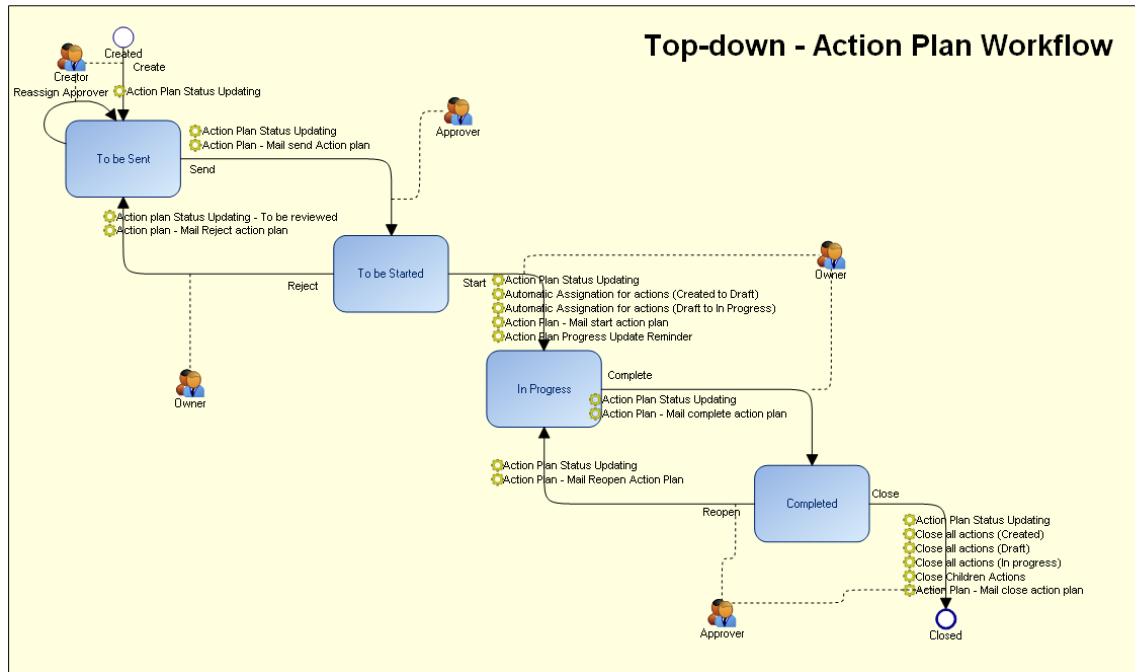
ACTION PLAN WORKFLOWS

- For more information on action plans, see [Using Action Plans](#).

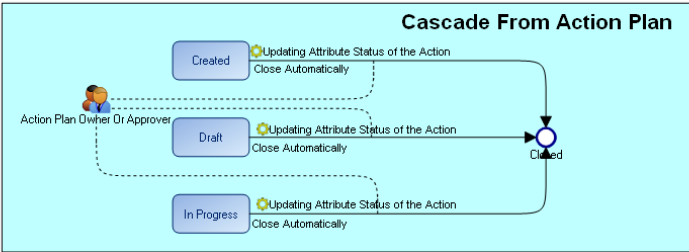
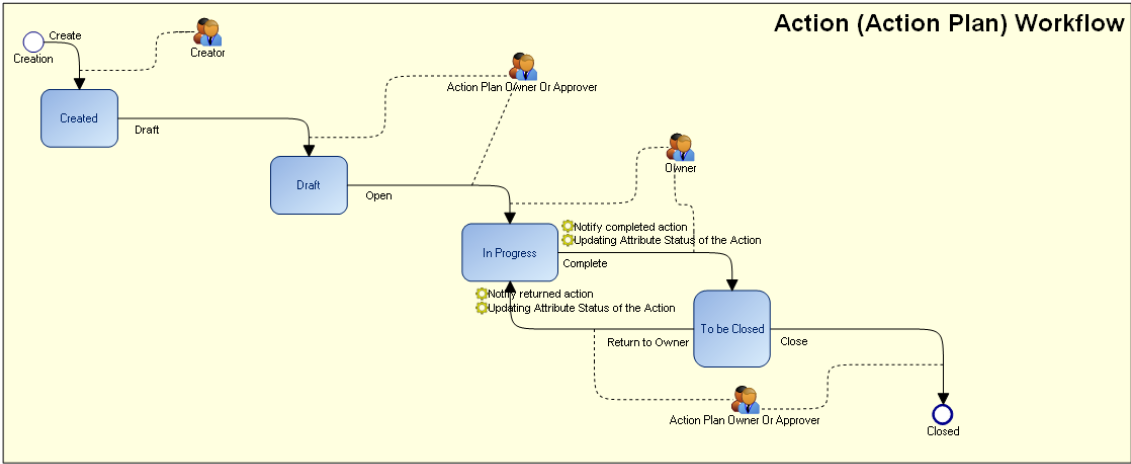
"Bottom-up" Action Plan Workflow



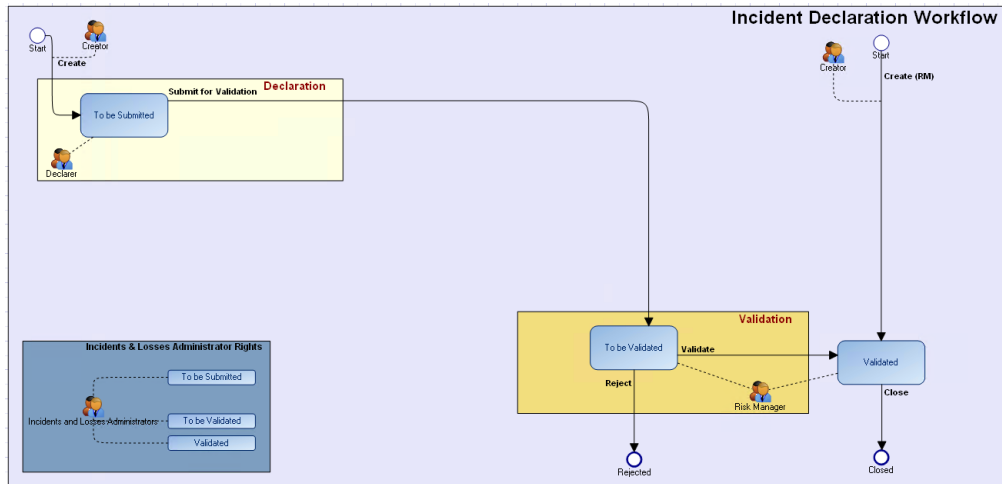
"Top-down" Action Plan Workflow



Action Workflow



INCIDENT WORKFLOW



- For more details on incidents, see [Incident Management Process](#).

HOPEX Internal Control



CONTENTS



Contents	1
---------------------------	----------

Introduction to HOPEX Internal Control	9
---	----------

Internal Control Process	10
<i>Control Library Definition</i>	10
<i>Control Execution</i>	10
<i>Control Assessment</i>	11
<i>Issue and Action Plan Management</i>	11
Accessing HOPEX Internal Control	12
Connecting to the solution	12
HOPEX Internal Control Profiles	12

Managing Controls	13
------------------------------------	-----------

Creating Controls	14
Control Characteristics	15
General characteristics	15
<i>Code</i>	15
<i>Control objective</i>	15
<i>Owner</i>	15
<i>Key control</i>	15
<i>Control nature</i>	15
<i>Operational cost</i>	15
<i>Execution mode</i>	16
<i>Status</i>	16
Scope of a Control	16
Responsibilities concerning Controls	16
<i>Responsibility levels</i>	16
<i>Specifying control responsible users</i>	17

Control Dashboard	17
Regulatory Enforcement	18
<i>Implemented control directives</i>	18
<i>Enforced regulation articles</i>	19
Accessing controls	20
Listing Controls	20
Accessing Controls by Control Types	20
Accessing Controls by Mitigated Risks	21
Accessing Controls by Implementation	21
Accessing Controls by Controlled Elements	21
Accessing Controls by Deficiencies	21
Contextualizing Controls	23
<i>Connecting processes to an entity</i>	23
<i>Connecting processes to a control</i>	23
Visibility of Controls	24
<hr/>	
Assessing controls	25
Control Assessment Types	26
Control Direct Assessment	27
Direct Assessment Context	27
Assessing a Control	27
Assessing Multiple Controls Simultaneously	28
Displaying the Results of Control Assessment	32
Analyzing Control Assessment Results	33
Instant reports	33
Dedicated analysis reports	33
Computing Assessment Results	34
<hr/>	
Executing controls	35
Preparing Control Execution	36
Defining Questions on Controls	36
Defining Control Execution Calendars	36
<i>Specifying a control steering calendar</i>	36
<i>Creating and configuring a steering calendar</i>	37
Defining Respondents	37
Connecting Controls to Entity Processes	38
Execution Campaign Principle	39
Preparing Execution Campaigns	39
Control Execution Periodicity	39
Assessment Template Specific to Control Execution	39
Creating Execution Campaigns	41
<i>Creating Execution Campaigns</i>	41
<i>Previewing the execution campaign</i>	43

Starting Execution Campaigns	44
Starting Execution Campaigns	44
Examples of Session Automatic Launch	44
Scheduling Execution Campaigns	46
Completing Control Execution Check-Lists	47
Managing Execution Check-Lists	48
Accessing Check-Lists	48
Following Check-Lists Up	48
<i>Campaign results</i>	48
<i>Check-list reports</i>	48
<i>Displaying check-lists measures</i>	48
<i>Displaying the aggregated measures</i>	48
Control Execution Reports	50
Detailed Execution Results	50
<i>Access path</i>	50
<i>Parameters</i>	50
<i>Result</i>	50
Consolidated Execution Results	50
<i>Access path</i>	50
<i>Parameters</i>	51
<i>Result</i>	51
Following Up Execution Sessions	51
<i>Access path</i>	51
<i>Availability</i>	51
<i>Parameters</i>	52
<i>Result</i>	52
 Control Testing	 53
Preparing Control Testing	54
Defining Test Sheet Questions	54
<i>Initializing testing steps</i>	54
<i>Creating testing steps</i>	54
Defining the Testing Method	55
Managing Teams	55
<i>Creating Controllers</i>	55
<i>Creating skill types</i>	55
<i>Creating skills</i>	56
<i>Creating skill levels</i>	56
<i>Defining skills for each user</i>	56
<i>Viewing skills</i>	57
Managing Currencies	58
<i>Defining Central Currency</i>	58
<i>Defining Local Currency</i>	59
<i>Modifying User Local Currency</i>	59
<i>Managing Exchange Rates</i>	59
Configuring Time Sheets	60
Managing Campaign Calendars	60
<i>Creating Calendars</i>	60

<i>Creating Calendar Periods</i>	61
<i>Connecting a Calendar to a Test Plan</i>	61
Preparing Tests	62
Creating a Test Plan	62
Planning Tests	63
<i>Creating a test</i>	63
<i>Accessing tests.</i>	63
<i>Defining test properties.</i>	63
<i>Creating "template" tests</i>	65
<i>Selecting tests to be executed</i>	65
<i>Selecting tests to be integrated in the test plan</i>	67
<i>Planning tests using a Gantt chart</i>	67
<i>Assigning resources to tests.</i>	68
<i>Sending the Notification Letter.</i>	69
<i>Validating tests</i>	70
<i>Publishing tests</i>	70
Preparing Tests.	70
<i>Work program creation prerequisites</i>	70
<i>Work program content</i>	71
<i>Creating work programs automatically</i>	71
<i>Completing the work program manually</i>	72
<i>Assigning activities</i>	73
<i>Reviewing the Work Program</i>	73
<i>Validating work programs</i>	74
<i>Executing administrative tasks.</i>	75
Executing Tests	76
Consulting the Work Program.	76
Executing Tests on Samples.	76
<i>Creating workpapers.</i>	76
<i>Specifying or modifying the sample size</i>	77
<i>Generating the test sample</i>	77
<i>Defining test sheet questions.</i>	77
<i>Completing the generated test sheets.</i>	78
<i>Assessing test activities.</i>	78
Assessing Controls	78
<i>Generating questionnaires.</i>	78
<i>Responding to Questionnaires</i>	79
Managing Time and Expenses.	79
<i>Managing expenses</i>	79
<i>Entering vacations</i>	80
<i>Completing a Time Sheet</i>	80
Management of issues and action plans.	81
<i>Managing issues.</i>	81
<i>Managing action plans.</i>	81
Supervising Tests	82
<i>Test check reports</i>	82
<i>Time sheet follow-up reports</i>	82
<i>Test expenses reports.</i>	83
Concluding Tests.	83
<i>Test assessment reports</i>	83
<i>Generating test reports.</i>	84
<i>Assessing tests.</i>	84

Terminating tests	84
Closing tests	84
Test Follow-Up	85
Implementing Action Plans	85
Accessing action plans	85
Implementing actions.	85
Action plan implementation follow-up.	85
Action Plan Follow-Up.	86
Test Plan Follow-Up	86
Displaying test plan follow-up reports.	86
Closing a test plan	87
Dashboard	87

Reports Related to Controls 89

Control Library Reports	90
Control Identification	90
Access path.	90
Parameters	90
Results	91
Control Location Matrix	91
Access path.	91
Parameters	91
Control Map.	92
Generating the control map	92
Control map content	92
Control Execution Reports	93
Detailed Execution Results	93
Access path.	93
Parameters	93
Result	93
Consolidated Execution Results	93
Access path.	93
Parameters	94
Result	94
Following Up Execution Sessions	94
Access path.	94
Availability	95
Parameters	95
Result	95
Control Assessment Reports.	96
Campaign Result Tree.	96
Access path.	96
Parameters	96
Campaign Result Matrix By Entity	96
Access path.	96
Parameters	97
Aggregation Report	97
Access path.	97

<i>Parameters</i>	97
Assessment Follow-Up Reports.	98
Session Follow-Up.	98
<i>Access path</i>	98
<i>Parameters</i>	98
Session Statistics	98
<i>Access path</i>	98
<i>Parameters</i>	98
<i>Result</i>	99
Control Testing Reports	100
Testing Coverage	100
Plan Synthesis	100
<i>Access path</i>	100
<i>Result</i>	100
Other Reports.	100
<i>Test plan follow-up reports</i>	101
<i>Test follow-up report</i>	101
<i>Action plan report.</i>	101
Issue Follow-up Reports	102
<i>Access path</i>	102
<i>Result</i>	102
<hr/>	
Managing Issues and Action Plans	103
Managing issues	104
Automatic Issue Creation.	104
Creating an Issue Manually	104
Remediating Issues.	104
Following Up Issues.	105
<i>Viewing remediated / non-remediated issues.</i>	105
<i>Generating issue follow-up reports</i>	105
Managing Action Plans for Internal Control	106
Creating Action Plans	106
Characterizing Action Plans	106
<i>General characteristics</i>	107
<i>Financial assertion</i>	107
<i>RACI.</i>	108
<i>Success factors</i>	108
<i>Scope?</i>	108
<i>Milestones</i>	108
<i>Attachments</i>	108
Managing Actions	108
<i>Creating Actions.</i>	109
<i>Defining action scope</i>	109
Action Plan Workflows	109
<i>"Bottom-up" approach</i>	109
<i>"Top-down" approach</i>	110
<i>Action workflow</i>	110
Indicating Action Plan Progress.	110

Action plan follow-up reports	110
<i>Access path</i>	111
<i>Result</i>	111

Using HOPEX UCF 113

About Unified Compliance Framework 114

Main Concepts Used in UCF	114
<i>Authority Documents</i>	114
<i>Citations</i>	114
<i>UCF Controls</i>	114
<i>Links between UCF concepts</i>	115

Building a Shared List	115
----------------------------------	-----

Mapping and Concepts 117

Mapping between UCF and HOPEX Concepts	117
Definitions of Main Concepts Used in HOPEX UCF	117

Managing UCF Environment in HOPEX UCF 119

UCF Import Prerequisites	119
Parameterizing UCF Import	119
Importing Data from the Common Controls Hub	120
Declaring Regulation Content as Relevant	121
<i>Regulatory content relevance</i>	121
<i>Reviewing regulatory frameworks after UCF import</i>	121
<i>Selecting relevant content for your organization</i>	121

Accessing your Control Framework Library 123

Viewing Regulatory Frameworks	123
<i>Accessing regulatory frameworks</i>	124
<i>Regulatory framework overview & description</i>	125
<i>Regulation articles of a regulatory framework</i>	125
Viewing Regulation Articles	126
<i>Accessing Regulation Articles</i>	126
<i>Viewing the objects subjected to a regulation article</i>	127
<i>Enforcement of a regulatory article</i>	128
<i>Connecting Business Documents</i>	128
Viewing Control Directives.	128
<i>Accessing control directives</i>	129
<i>Viewing fulfilled regulation articles</i>	129
<i>Supported and supporting directives</i>	130
<i>Enforcement level of control directives</i>	132
<i>Viewing HOPEX controls implementing a control directive</i>	132
<i>Connecting Business Documents</i>	133

INTRODUCTION TO HOPEX INTERNAL CONTROL



HOPEX Internal Control is an internal control management solution covering the different phases of internal control. This solution enables:

- 6 definition of internal control systems with creation of a control library
- 6 execution of controls
- 6 assessment of controls, directly or by assessment campaigns or tests
- 6 management of issues and action plans

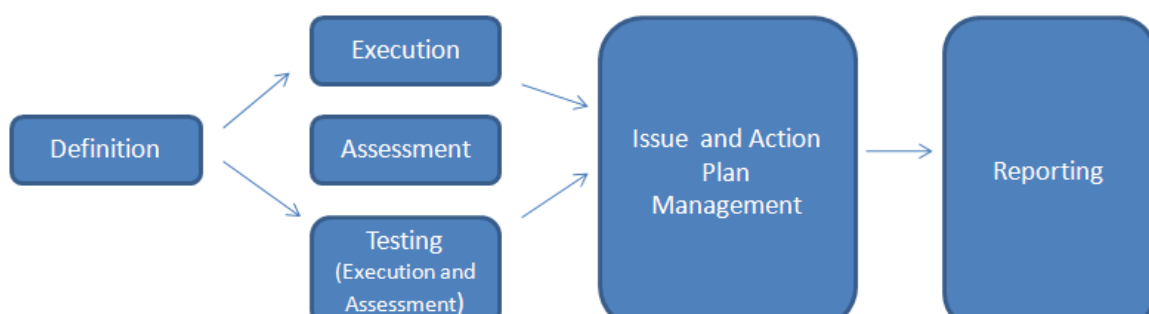
HOPEX Internal Control is intended for internal control managers, internal controllers and business process managers. An interface customized according to profile accompanies implementation of internal control systems.

INTERNAL CONTROL PROCESS

Internal control consists of checking that controls carried out during enterprise processes have been correctly executed and are efficient.

HOPEX Internal Control covers the different phases of internal control:

- Control Library Definition
- Control Execution
- Control Assessment
- Control Testing
- Issue and Action Plan Management



Defining the internal control library is a prerequisite for control execution and assessment activities.

Execution and assessment of controls can be carried out independently.

- *Reporting functions are available at all times, either globally or for each internal control step.*

Control Library Definition

HOPEX Internal Control allows internal control managers to:

- identify controls
- contextualize controls in the company repository, that is to connect them to the appropriate processes and entities

See [Managing Controls](#).

Control Execution

Controls are regularly executed by managers to check that first level controls are correctly executed. **HOPEX Internal Control** allows:

- creation of questionnaires called check-lists
- definition at regular intervals of control execution campaigns
- follow-up and consolidation of control execution results from reports

- *The **HOPEX Internal Control** solution does not concern first level controls executed by operational management during execution of enterprise processes.*

See [Executing controls](#).

Control Assessment

Assessment of relevance of controls in terms of design and efficiency can be carried out by means of:

- assessment campaigns via questionnaires
See [Managing Assessment Campaigns](#).
- direct assessment
See [Assessing controls](#).
- control tests organized by the internal control department
See [Control Testing](#).

Issue and Action Plan Management

Issues can be identified from control assessment questionnaires or specified directly in the solution.

Resolution of issues is formalized by implementation of action plans. Reports assure efficient follow-up of internal control activities.

See [Managing Issues and Action Plans](#).

ACCESSING HOPEX INTERNAL CONTROL

The menus and commands available depend on the profile with which you are connected.

Connecting to the solution

For connect to HOPEX, see **HOPEX Common Features**, "HOPEX desktop", "Accessing HOPEX (Web Front-End)".

- For more details on how to use the interface, see the **HOPEX Common Features** guide.

HOPEX Internal Control Profiles

In **HOPEX Internal Control**, there are, by default, business profiles with which specific activities are associated.

Profiles	Desktop	Tasks
Internal Control Director (Or GRC manager)	HOPEX IRM	<ul style="list-style-type: none"> - Have all rights on workflows, objects and menus of the solution - Validate campaigns - Prepare test plans - Validate action plans
Internal Controller (Or GRC manager)	HOPEX IRM	<ul style="list-style-type: none"> - Define controls - Prepare campaigns - Execute tests (create work programs, create issues and action plans) - Validate and follow up action plans
GRC Contributor (Lite)	IRM Contributors	<ul style="list-style-type: none"> - Complete control execution check-lists - Answer assessment questionnaires - Define and create action plans (and create issues) <p>See The IRM Contributor Desktop.</p>

MANAGING CONTROLS



HOPEX Internal Control enables creation of control libraries and connection of controls to objects in their environment. This enables positioning of controls in their business context. This "contextualization" allows internal control managers to define adapted controls and subsequently carry out relevant assessments.

- 6 [Creating Controls](#)
- 6 [Control Characteristics](#)
- 6 [Accessing controls](#)
- 6 [Contextualizing Controls](#)
- 6 [Visibility of Controls](#)

CREATING CONTROLS

The GRC Manager, the internal controller, the internal control director and the functional administrator can create controls.

To create a control:

1. In the **HOPEX IRM** desktop, select **Libraries > Control Library > All Controls**.
2. Click **New**.
The control created appears in the list of controls. You can now specify the various characteristics from the properties window.
 - For more details, see [Control Characteristics](#).

CONTROL CHARACTERISTICS

Different sections are available in the properties of a control.

- To access controls, see [You can access controls through lists and trees which allow classification of controls according to different criteria..](#)

General characteristics

Code

The code enables unique identification of the control.

Control objective

You can enter a comment describing the required objective of setting up the control.

Owner

The control owner is the user responsible for execution of the control.

This field is used when there is only one "Responsible" (in the RACI sense).

- For more details on RACI, see [Responsibilities concerning Controls](#).

Key control

When the **Key control** check box is selected, the control appears in the following list:

Libraries > Control Libraries > All Controls > Key Controls

Control nature

This characteristic allows you to specify the nature of the control. You can select from three main internal control types:

- Corrective
- Detective
- Preventive

Operational cost

This characteristic enables indication of a control cost assessment.

Execution mode

This characteristic enables specification of how the control is carried out:

- "Automatic"
- "Manual"
- "Semi-automatic"

Status

- "Draft"
- Validated

Scope of a Control

The **Scope** section of control properties enables connection of controls to other objects:

- Business processes
- Organizational processes
- Entities
- Risks
- Accounts
- Requirements
- Types of control

Responsibilities concerning Controls

HOPEX Internal Control enables definition of responsibilities of each participant related to a control via the RACI matrix:

- Responsible
- Accountable
- Consulted
- Informed

Responsibility levels

The proposed responsibility levels are as follows:

Responsibility	Meaning
Responsible	Responsible for execution of required actions.
Accountable	Reporting on progress of planned actions and making decisions. There is only one "Accountable".
Consulted	Consulted as first priority before an action or decision.
Informed	Must be informed after an action or decision.

Specifying control responsible users

In the framework of control assessment via campaigns, questionnaire respondents are **Responsibles** of control.

- For more details on assessment campaigns, see [Managing Assessment Campaigns](#)

You can connect several "Responsible" users for the same control in different entities.

To specify the person responsible for a control in a given entity:

1. In the control properties page, expand the **Responsibilities** section.
 - To access controls, see [Listing Controls](#).
2. Select the **Responsible** tab.
3. Click the **Connect** button.
In the dialog box that appears, click the **Find** button.
4. Select a person in the list that appears and click **Connect**.
The person appears under the tab concerned. You must now connect the person to an entity.
5. In the **Assignment Location** field, select an entity to which the person executing the control is attached.
 - Ensure that an e-mail address is correctly specified in the properties of the person.

Control Dashboard

In the upper part of a control property page, a dashboard displays indicators.

Assessment Freshness

This indicator enables to know when the last assessment was performed.

Aggregated Execution Rate

The aggregated execution rate concerns control execution checklists. For more details on this functionality, see [Executing controls](#).

For example:

If controllers assessed 70% of controls in a specific context, 50% in a an another, and 20% in another, the gross execution rate on the control is 46.6%.

Open Issues

Open issues are issues for which the action plan was not completed.

For more details, see [Managing Issues and Action Plans](#).

Aggregated Pass Control Level

Aggregated Pass Control Level = Control Design (IC) * Control Efficiency (IC)

As a reminder, these are the possible values used to compute the Pass Control Level:

- Control Design:
 - Pass
 - Fail
- Control Effectiveness:
 - effective
 - ineffective

Regulatory Enforcement

If you have **HOPEX UCF**, the property pages of controls display the **Regulatory Enforcement** section.

– For more information about **HOPEX UCF**, see [Using HOPEX UCF](#).

Two tabs are displayed:

- **Implemented control directives**
- **Enforced regulation articles**

Regulatory Enforcement		
Connect	Implemented Control Directives	Enforced Regulation Articles
Name ↑	Enforcement Level	Control Nature
Report data loss event informatio...	Mandated Control	Corrective

Implemented control directives

You can view or specify which control directives your control implements (to help contribute to the enforcement of any regulation article).

Enforced regulation articles

You can view which regulation article your control is actually implementing (through control directives).

ACCESSING CONTROLS

You can access controls through lists and trees which allow classification of controls according to different criteria.

Listing Controls

To list all controls:

- > In the **HOPEX IRM** desktop, select **Libraries > Control Library > All Controls**.

A drop-down list enables to refine control access and classification according to different criteria:

- Key Controls
 - *Key controls are the controls for which the **Key control** check box has been selected in the control properties.*
- Controls with Failed Execution
 - *This list displays controls with an aggregated execution rate lower than 90%. For more details on aggregated execution rate, see [Control Dashboard](#).*
- Controls with Low Pass Control Level
 - *This list displays controls with an average pass level lower than 85%.*
 -) *Control level characterizes efficiency level of control elements deployed (controls) to assess the risk.*
- Risks without Recent Assessment
 - *This list displays controls which have not been assessed for at least 12 months.*

Accessing Controls by Control Types

To access controls through a tree of control types:

- > In the **HOPEX IRM** desktop, select **Libraries > Control Library > All Controls > By Taxonomy**.
 -) *A control type allows the classification of controls implemented in a company in accordance with regulatory or domain specific standards (Cobit, etc.).*

Accessing Controls by Mitigated Risks

To view controls which mitigate (or not) risks:

- › In the **HOPEX IRM** desktop, select **Libraries > Control Library > All Controls > By Mitigated Risks**.

A drop-down list enables to distinguish between:

- Controls mitigating risks
- Controls not mitigating Risks

Accessing Controls by Implementation

You can create action plans to implement or modify controls.

To access controls according to their implementation status:

- › In the **HOPEX IRM** desktop, select **Libraries > Control Library > All Controls > By Implementation**.

A drop-down list enables you to view:

- controls associated with an action plan.
- controls associated with a delayed action plan.

For each control, columns display:

- If the control is a key control
- The control nature (preventive, corrective)
- The number of implementation action plans

Accessing Controls by Controlled Elements

Trees display controls classifying them by objects the controls apply to:

- processes
- entities
- applications
- accounts

A tree also gives the possibility to view the controls which are not associated to an object.

Accessing Controls by Deficiencies

A drop-down list enables to view controls linked to:

- Open Issues
- Incidents (controls with mitigated and materialized risks)

In the list of controls linked to incidents, the following is displayed in column:

- the number of incidents
- the date of the last incident occurrence
- total net loss

CONTEXTUALIZING CONTROLS

The same control can be assessed in the framework of different contexts (for example processes or entities). To enable this multiple assessment, you must "contextualize" controls, that is connect them to context objects.

You must **connect controls to entities through the indirect link "Control->Process->Entity"**:

- Connect processes (organizational or business) to entities of the organization.
 - See [Connecting processes to an entity](#).
- Connect controls to processes
 - See [Connecting processes to a control](#).

Connecting processes to an entity

To connect processes to an entity:

1. In the navigation menu, select **My Environment > My Organization > My Entities** and select an entity.
2. In the properties of the entity, expand the **Scope** section.
3. In the subtab corresponding to organizational or business processes, click **Connect**.
4. In the query dialog box that appears, click the **Find** button, select the required process and click **Connect**.

Connecting processes to a control

To connect processes to a control:

1. In the navigation menu, select **Libraries > Control Library > All Controls**.
2. In the control property page, select the **Characteristics** tab and expand the **Scope** section.
3. In the subtab corresponding to organizational or business processes, click **Connect**.
4. In the query dialog box that appears, click the **Find** button, select the required process and click **Connect**.

VISIBILITY OF CONTROLS

By default, controls are visible to all. However, you can modify only those controls attached to your reference entity or to one of its sub-entities.

- *A user is connected to a reference entity in the framework of his/her assignment. For more details on assignments, see chapter "Managing Users" in the **HOPEX Power Supervisor** guide.*

If according to your assignment you are connected to the "France" entity, you cannot modify controls that have "World" entity context.

However, if you are connected to the "World" entity, you can modify controls that have "France" entity context.

ASSESSING CONTROLS



Controls can be assessed in terms of their design/efficiency. Assessment can be carried out directly on controls or remotely via questionnaires.

- *This chapter explains how to start assessments.*

*To configure these, see [Assessment Templates](#) in the **HOPEX Power Studio** - Assessment documentation.*

- *The results of the control assessment can be presented in dedicated reports that facilitate the analysis of the controls assessed. For more details, see [Control Assessment Reports](#).*

- 6 [Control Assessment Types](#)
- 6 [Control Direct Assessment](#)
- 6 [Analyzing Control Assessment Results](#)
- 6 [Computing Assessment Results](#)

CONTROL ASSESSMENT TYPES

An assessment is designed to give values, in a specific context, to the different characteristics of a control.

Characteristics values can be specified:

- From the control properties page: see [Assessing a Control](#).
- From a multiple assessment table: see [Assessing Multiple Controls Simultaneously](#).
- Through an assessment questionnaire sent to appropriate recipients: see [Risk and Control Campaign Assessment](#).
 - **HOPEX IRM** also allows internal controllers and auditors to assess questionnaires on site. For more details, see [Control Testing](#).

CONTROL DIRECT ASSESSMENT

HOPEX IRM enables assessment of controls in terms of design and efficiency:

You can assess controls:

- Directly
- Through questionnaires sent to identified recipients.
 - For assessment by questionnaire, see [Managing Assessment Campaigns](#).

Direct Assessment Context

In direct assessment, the values of the control characteristics can be specified in two ways:

- In the properties of each control
- globally, using a multiple assessment table.

This is an "expert view" assessment.

- You can assess controls for which you have editing rights.

Direct assessment is carried out for all context objects available in the **Scope** section of control properties:

- Organizational processes
- Business processes
- Entities
 - For more details on control contextualization see also [Contextualizing Controls](#).

Assessing a Control

- Before assessing a control, you need to ensure it has been contextualized in an appropriate way. For more details, see [Contextualizing Controls](#).

To directly assess a control:

1. Open the properties of a control.
2. In the **Assessment** page, click **Perform Assessment**.
 - The **Perform Assessment** is available if the control has been contextualized accordingly (a control must be connected to a process, which must in turn be connected to an entity).
3. In the wizard that appears, select the context(s) to be included in the control assessment.

4. Click **Next**.
You can now select values that characterize this control (contextualized) in terms of:
 - design
 - effectiveness
 - *Other questions can be asked if your administrator has configured the questionnaire supplied as standard.*
5. In the **Control Design** and **Control Effectiveness** fields, indicate whether the control is:
 - Pass
 - Fail
 - *Values are applied to all previously selected assessment nodes.*
6. Specify the measure date in the calendar.
By default this is today's date. You can select a date earlier than today's date.
7. Click **OK**.
Control measures are created for each assessment node (ie. the control in a particular context).

You can create several measures on different dates in the same way.

Assessing Multiple Controls Simultaneously

If you have to assess several controls, it can be quicker to use the multiple assessment table. This table allows you to specify the same value for several assessment nodes of different controls.

- *An assessment node comprises:*
 - *an object to assess*
 - *one or several context objects (entities, processes, operations), if necessary*

To assess multiple controls simultaneously:



1. From the navigation menu click **Assessment > Direct Assessment > Control Multiple Assessment Table**.
2. In the window that appears, click **Launch Multiple Assessment**.


3. Select the type of object that constitutes the context for controls:

- Org Unit
- Operation
- Business processes
- Organizational Process

The control assessment template is selected by default.


Multiple Assessment - Select Context Element & Template

 To build a new Multiple Assessment Table, first select the relevant context element.


Context Element

Org-Unit
▼

 Select the relevant assessment template. Available options are determined by the previously selected context element.

Assessment Template *

Control Assessment
▼

 Assesses Controls in the combined context of Entities, Business & Organizational Process and Operations using the following criteria:

- Design
- Effectiveness

4. Click **Next**.

5. In the displayed tree, select the objects that apply to the context.
A control is assessed in the context of elements of the branch from the control up to the root.

Multiple Assessment - Select Assessed Objects

The context(s) corresponding to your previous selection are presented below in a hierarchy. You can expand the hierarchy and select either a whole set of contexts or a single context. All objects applying to these selected contexts will be included into your multiple assessment table unless you deselect them.

Controls by Entity :

Select parents and sub-elements | Expand the selected items

Administration department

Governance Process

Media Library Flat Model

Production Process

Car Rental Business

Car Rental Supporting Process

Car Movement

Vehicle Repair

Account Management

Body Problem Overview

Previous

Next

OK

Cancel

In the above example, if you select the "Car Rental Business" process, all controls 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.

6. Click **OK**.
The list of controls to be assessed in a particular context appears.
7. Answer the questions for each context and indicate whether the control design and effectiveness is:
 - Pass
 - Fail
8. Click **OK**.

An assessment is automatically created in the **Assessment** page of the control properties. For more details, see [Displaying the Results of Control Assessment](#).

DISPLAYING THE RESULTS OF CONTROL ASSESSMENT

To display the results of assessments performed on a control:

1. From the control library, select the **Assessment** page of the control properties.
2. (optional) In the **Assessment Results** section, select the context element and template you are interested in and click **Apply filters**. The corresponding assessments appear. This way you can filter assessments when there are a lot of them.

The **Control Level** (Pass/Fail) is automatically calculated from the specified characteristics values.

See also: [Computing Assessment Results](#).

ANALYZING CONTROL ASSESSMENT RESULTS

Instant reports

Instant reports offer a statistical graphic analysis of the data. You can generate instant reports on a selection of assessments in order to view certain data graphically or to compare the assessments for specific characteristics.

To launch an instant report on a set of assessment of a control:

1. Display the properties of the control and click the **Assessment** page.
2. Select the assessments in question.
3. Click the **Instant Report** button.
4. Select the type of report to create and then, if necessary, the characteristics to be analyzed.

For more details on instant reports, see the HOPEX Common Features user guide, "Generating Documentation", "Managing Instant Reports".

Dedicated analysis reports

In addition to instant reports, **HOPEX IRM** provides dedicated report templates that facilitate the analysis of the assessed controls. For more details, see [Assessment Follow-Up Reports](#).

COMPUTING ASSESSMENT RESULTS

Metaattribute	Computed / Not Computed	Explanations
Control Design (IC)	Computed through the [Internal Control - Control Attributes] macro	<ul style="list-style-type: none"> - if assessment node, value computed from the assessed characteristic "Control Design" (IC). - if aggregation node, value computed from the assessed characteristic "Average percentage of Pass Control Level".
Control Effectiveness (IC)	Computed through the [Internal Control - Control Attributes] macro	<ul style="list-style-type: none"> - if assessment node, value computed from the assessed characteristic "Effectiveness". - if aggregation node, value computed from the assessed characteristic "Average percentage of Pass Control Level".
Control level (IC)	Computed through the [Internal Control - Computed Control Attributes] macro	Rounded result obtained from the formula: Control Design (IC) * Control Effectiveness (IC)
Control Execution Value (IC)	Not computed	

- For more details on aggregation, see [Aggregation Schemas](#) in the **HOPEX Power Studio** - Assessment documentation.

EXECUTING CONTROLS



Controls are executed periodically by process managers, to check that operational processes have been executed correctly and that their results comply with expectations.

Controls are executed in their context, by process and entity. They are presented in the form of check-lists. These check-lists are questionnaires presenting questions on each control. You can create your own questions, for all controls or for specific controls.

Automatically generated reports allow control execution progress follow-up and consolidation of results.

- 6 [Preparing Control Execution](#)
- 6 [Execution Campaign Principle](#)
- 6 [Creating Execution Campaigns](#)
- 6 [Starting Execution Campaigns](#)
- 6 [Completing Control Execution Check-Lists](#)
- 6 [Managing Execution Check-Lists](#)
- 6 [Control Execution Reports](#)

PREPARING CONTROL EXECUTION

To be able to start execution campaigns, you must first:

- define control steps on each control
See [Defining Questions on Controls](#).
- specify a steering calendar on controls to be assessed
See [Defining Questions on Controls](#).
- define check-list respondents
See [Defining Respondents](#).
- connect processes to controls to be executed
See [Connecting Controls to Entity Processes](#).
 - See also [Contextualizing Controls](#).

Defining Questions on Controls

Before starting execution campaigns, you must define the content of check-lists used at control execution. It consists in defining questions to ask when executing controls.

You can for example define questions that have "OK/KO" as an answer. For more details on question types, see [Question Types](#).

- Only answers of type "OK/KO" can be aggregated in execution campaign results. Other answer types are considered for information only.

To create questions on a control:

1. In the control properties, select the **Execution** page.
2. In the **Control Steps** section, click the **Create a Questionnaire Template** button.

The questionnaire creation tool opens. For more information on how to use it, see [Questionnaire Templates](#).

Defining Control Execution Calendars

To define periodicity of control execution, you must specify the steering calendar to be used.

- You can specify the control execution steering calendar only after having created the questionnaire (that is to say control steps). See [Defining Questions on Controls](#).

Specifying a control steering calendar

To specify a steering calendar:

1. In the properties of a control, select the **Execution** page from the drop-down list.

2. Ensure you have properly created a questionnaire template.
 - See [Defining Questions on Controls](#).
3. Select an **Execution Frequency**.
 - *This field is for information only.*
4. Select a **Steering Calendar**.
Different steering calendars exist for different execution periodicities:
 - daily
 - monthly
 - weekly
 - *You can create a steering calendar if none of those supplied as standard is suitable.*

Creating and configuring a steering calendar

To create a steering calendar:

1. In the control properties, select the **Execution** page.
 - *Ensure you have properly created a questionnaire template. See [Defining Questions on Controls](#).*
2. Expand the **Execution Method** section.
3. In the **Steering Calendar** field, click **Create a steering calendar**.
4. In the wizard that opens, connect a **Steering Date** (which corresponds to the execution frequency of interest to you).
5. Open the steering date properties dialog box and select the **Scheduling** tab.
6. Specify the information required for starting the campaign including:
 - start and end dates for execution campaigns
 - *Begin and end dates specified on the steering calendar do constitute campaign start and end dates. They simply serve to define the interval within which assessment sessions can take place.*
 - *It is recommended to use a relative begin date on the steering date.*
 - start date and hour (defined in **UTC** format).
 - *For details on possible configurations, see the section concerning the scheduler in the technical article "HOPEX Studio".*
7. Select **Execute at start date & time** if you wish to launch the campaign execution immediately.
 - *If the check box is deactivated, the scheduler waits for the next recurrent date (and time) to trigger the job.*

Defining Respondents

On each control you must define persons responsible for completing execution check-lists. To do this, you must define control responsible users, that is "Responsible" in the RACI sense of the term.

To define respondents:

1. In the control properties, expand the **Responsibilities** section.

2. In the **Responsible** tab, connect a user and specify its location.

Responsibilities

Responsible Accountable Consulted Informed

New

Connect

Name	User Email	User Login	Assignment Location
------	------------	------------	---------------------

- For more details, see [RACI Responsibilities](#).

Connecting Controls to Entity Processes

Controls are executed in the framework of organizational/business processes, connected to organization entities.

To connect controls to processes, see [Contextualizing Controls](#).

EXECUTION CAMPAIGN PRINCIPLE

Preparing Execution Campaigns

To be able to create an execution campaign, preparatory work is required at the level of controls. You must:

- **connect processes to controls**
 - See [Contextualizing Controls](#).
- **define questions on controls**
 - For this you must define control steps (questionnaire templates).
- **define control execution calendars**
 - You must specify a steering calendar on each control to execute. See [Defining Control Execution Calendars](#).
- **define check-list respondents**, who are control owners for a specific entity.
 - See [Defining Respondents](#).

Control Execution Periodicity

An execution campaign groups several execution sessions.

Each campaign session groups a set of controls to be executed on the same date.

Several assessment sessions are created in parallel for each steering calendar type identified.

For example:

a session is created each week if a weekly steering calendar has been specified on certain controls

a session is started each day if a daily steering calendar has been specified on certain controls

Controls are therefore grouped in each session according to the steering calendar to which they have been connected.

See also: [Examples of Session Automatic Launch](#).

Assessment Template Specific to Control Execution

Execution campaigns are automatic assessment campaigns with a specific assessment template.

The "Control Execution" assessment template is selected by default at execution campaign creation. This assessment template:

- prompts you to specify an entity.
- is used to identify controls used by processes attached to this entity and its sub-entities.

Check-list respondents are control owners in an entity or in sub-entities.

CREATING EXECUTION CAMPAIGNS

The execution campaign creation wizard enables definition of campaign scope.

Creating Execution Campaigns

To create an execution campaign:

1. In the **HOPEX IRM** desktop, select **Execution > Campaigns**.
2. Click **New**.
3. In the creation window that appears, modify the proposed dates if necessary.

The campaign **Begin Date** marks the start of the execution campaign.

- The "Control Execution" assessment template is selected by default. For more details, see [Assessment Template Specific to Control Execution](#).

Creation of Assessment Campaign - Properties

Local name

Assessment Campaign-1

Assessment Campaign Owner*

GLEVER Herveline

Assessment Template

Control Execution

Calendar*

2020

Begin Date*

12/16/2020 

End Date*

12/31/2020 

4. Click **Next**.
You will now define the scope of your execution campaign.

5. In the **Assessed Parameters** field, find the root entity that interests you, using the arrows on the right of the field.

Creation of Assessment Campaign - Preview & Parameters

Local name

Assessment Campaign-1

Assessed Parameters

Root Entity

World@Hand Corporation

Refresh the report

Excel Export File Name

Information

Assessment Campaign	Assessment Campaign-1
Description	
Assessment Campaign Code	
Campaign Type	Execution

6. In the preview window, click **Refresh the Report**.
Elements concerning the assessment campaign appear:
- general information: for example begin and end dates, person responsible, number of objects to be assessed, number of respondents, number of contexts
 - assessed objects (controls)
 - context objects (entities and organizational/business processes)
 - respondents
 - Respondents execute controls. For more details on control responsibilities, see [Responsibilities concerning Controls](#).
 - assessment nodes, presenting objects to be assessed in their context, with specified respondent
 - If no respondent has been specified on the control, or if no e-mail address is associated with the respondent, a red frame appears before the assessment node.
7. Click **OK**.
The campaign appears in the list.

Previewing the execution campaign

To preview execution campaign scope, before launching the campaign:

- > Open the properties of the campaign and select the **Preview and Parameters** page.

You can check data such as respondent, email, control scope. If data seems incorrect or incomplete, you can modify it before starting the campaign.

- *For a reminder on work control execution preparatory work, see [Preparing Control Execution](#).*

STARTING EXECUTION CAMPAIGNS

When you have created the execution campaign, you must start it via the workflow.

Starting Execution Campaigns

To start the execution campaign:

1. In the **HOPEX IRM** desktop, select **Execution > Campaigns**.
2. Click the campaign icon and select **Automatic Assessment Campaign (In Preparation) > Start**.

- "(In Preparation)" corresponds to the current status of the automatic execution campaign.

The campaign is started automatically:

- on the begin date specified on the campaign
- at the time indicated on the steering calendar

Start of the execution campaign invokes automatic processing enabling planning and start of sessions.

- A message indicating that parameterization is not complete might appear. This is the case when controls of scope are not connected to a steering calendar. However you can start the campaign.

Examples of Session Automatic Launch

Execution sessions are started according to:

- execution campaign begin and end dates
 - begin and end dates and recurrences specified on the steering calendar of the controls to be executed
- For more details on steering calendars, see [Defining Control Execution Calendars](#).

When a due date is reached, **HOPEX** checks:

- that the campaign has not been closed manually
- that the campaign end date is not expired

If both conditions are met, the next session is scheduled.

Example 1

If the begin date specified on the steering calendar is later than the campaign end date, controls are not executed.

Example 2

On the steering date it is specified that execution is scheduled everyday at 6am.

The campaign is created and the transition is triggered at 10am.

If the check box **Execute at start date/hour** is not selected, the campaign is launched on the morrow at 6am.

- If the check box is selected, a message indicates scheduling in the past is not possible.

Example 3

The check box **Execute at start date/hour** is selected.

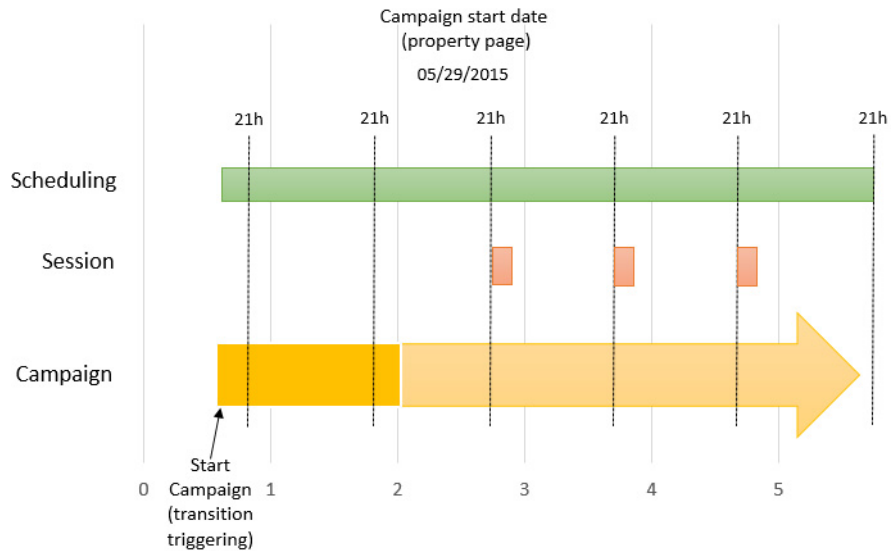
On the execution campaign, the date of the first scheduled execution is later than today's date (campaign start date).

In that case, the campaign start date corresponds to the launching of the assessment session.

Example 4

Example of scheduling on the steering calendar

The following result is obtained:



Scheduling Execution Campaigns

To consult dates and times of next execution of a campaign in progress:

1. In the **HOPEX IRM** desktop, select **Execution > Campaigns**.
2. Open the properties of the execution campaign and select the **Automatic Execution** page.

The list of timespots defined by the steering calendar appears.

The **End Date** indicated on the campaign defines the effective end of the campaign. For more details on sessions actually launched, see [Examples of Session Automatic Launch](#).

- The dates indicated correspond to the scheduled jobs. A new session is created at each job execution. The previous session is closed.

To view the sessions in progress, login with the "IRM Functional Administrator" profile and select **Administration > Tools > Scheduling Management**.

You may force the trigger of a job for testing purposes. To do so, in the **Triggers** section, select the session and click **Execute**.

COMPLETING CONTROL EXECUTION CHECK-LISTS

When the execution campaign has started, you can complete check-lists. To do this, you must connect with a user with the "GRC Contributor (Lite)" profile.

- For more details, see [Managing Questionnaires and Check-lists](#).

To complete the check-lists addressed to you:

1. In the "IRM Contributor" home page, click **My check-lists to complete**.
 - In the **HOPEX IRM** desktop, select **My Tasks > Execution > Check-lists To Complete**
2. Click the check-list to complete.
The check-list opens.
3. Select an object to assess from the list and answer the questions.
4. Select another object to be assessed and answer the questions.
 - If you want to continue and answer later, click **Save & Close**.
5. After answering all questions, click **Submit**.

MANAGING EXECUTION CHECK-LISTS

Accessing Check-Lists

You can view control execution check-lists at any time.

To access check-lists:

- > In the **HOPEX IRM** desktop, select **Execution > Follow-Up**.
From the drop-down list, you can view the check-lists which were:
 - sent in the framework of the campaign
 - completed by respondents
 - not yet completed

Following Check-Lists Up

Campaign results

For each executed control, **HOPEX IRM** calculates the percentage of "OK" steps in the total number of steps. This calculation is executed using an aggregation schema.

- "N/A" answers are excluded from the total number of steps. This rule can however be customized.

Check-list reports

Reports allow you to follow up check-list progress and results. For more details, see [Control Execution Reports](#).

Displaying check-lists measures

To view check-list measures as well as the corresponding questionnaires:

1. In the control properties, select the **Execution** page.
2. In the **Detailed execution results** section, right-click a node to display the questionnaire.

Displaying the aggregated measures

To display measures from aggregation nodes:

1. In the control properties, select the **Execution** page.
2. In the **Aggregated Execution Results** section, the list of aggregated measures appears.
 - Only the internal Control Director and the IRM Manager can view this list.

Example of Aggregated Execution Rate

If controllers have assessed:

- 70% of controls in one of the contexts
- 50% of controls in another context
- 20% of controls in a third context

=> the aggregated execution rate is 46,6%.

CONTROL EXECUTION REPORTS

To access control execution reports:

- > In the **HOPEX IRM** desktop, select **Analysis > Controls > Execution**. Different reports are available from the drop-down list.

Detailed Execution Results

This report presents results of each execution campaign session.

Access path

Analysis > Control > Execution > Detailed Execution Results

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Result

The report is presented as a table:

- in rows: tree of controls in their context
- in columns: results (control level)

-

Consolidated Execution Results

This report presents aggregated results of controls by entity and by month.

Access path

Analysis > Control > Execution > Consolidated Execution Results

Parameters

Parameters
calendar
Begin Date
End date
Entity type
Entity

Result

The matrix comprises:

- a list of entities: by default, all entities are selected.
 - *If the "Entity type" parameter is specified, selected entities correspond to this specified entity type.*
- a **Total number of controls**: number of controls linked to the entity (or its sub-entities).
- a **Total number of instances**: controls are counted as many times as there are contexts for the same control.

If a control is assessed in the framework of two different entities, the control is counted twice: **HOPEX IRM** distinguishes two instances of the assessed control.
- for each month:
 - a **Number of assessed instances**
 - a number of instances considered as satisfactory ("pass")
 - a % of instances considered as satisfactory ("pass")

Following Up Execution Sessions

This report enables follow-up of assessment sessions of "Execution" type.

Access path

Availability

This report is also available from a particular execution session.

To access this report from an execution session:

1. In the properties of an execution campaign, select the **Sessions** tab and open the properties page of an assessment session.
2. Select the **Reporting** tab, then **Follow-Up**.

Parameters

Parameters
Session

Result

A summary displays general information on the current session.

This report presents charts concerning campaign progress:

- Percentage of completed questionnaires
- Distribution of questionnaires by status
- Distribution of questionnaires delegated/not delegated
- Distribution of questionnaires by status, for each respondent
- Distribution of questionnaires by status, for each assessed object

CONTROL TESTING



Control tests can be carried out to complement operational management reviews. These tests consist of carrying out an internal audit on controls. **HOPEX Internal Control** allows internal controllers to:

- 6 execute tests on site by completing test sheets
- 6 assess these executed tests
- 6 assess controls in terms of design and efficiency by means of questionnaires.
- 6 implement action plans to improve controls for which issues have been identified
- 6 complete expense sheets and time sheets

The testing process consists of three phases:

- 6 [Preparing Control Testing](#)
- 6 [Preparing Tests](#)
- 6 [Executing Tests](#)
- 6 [Test Follow-Up](#)

PREPARING CONTROL TESTING

To prepare control testing by the internal control team, you must create questions that will be used to generate test sheets.

- See also [Contextualizing Controls](#).

Defining Test Sheet Questions

You must define testing steps on controls to be able to generate test sheets used by internal controllers.

To create testing steps:

1. In the control properties, select the **Test** page.
2. In the **Testing Steps** section click Create **Questionnaire Template**. The Questionnaire Builder opens.
3. Create questions as described in the paragraph [Inserting questions](#) of the Questionnaire Builder documentation.

Defining the Testing Method

- *To be able to define a testing method, you must first have created questions on the control.*

To specify control test characteristics:

1. In the control properties, select the **Testing** page.
The **Testing Method** section presents characteristics concerning testing.
2. Specify the **Testing Frequency**:
 - Yearly
 - Quarterly
 - Bi-Yearly
3. Specify the **Testing Method**:
 - Inquiry
 - Inspection
 - Observation
 - Re-performance
4. Specify the **Testing Population Size**: the total number of objects that could be controlled (for example: 1000 invoices or 100 contracts).
5. Specify the **Testing Sample Size**: value inherited by test sheets by default.

- *For more details, see [Specifying or modifying the sample size](#).*

Managing Teams

Before planning tests, appropriate teams must be set up and roles and responsibilities assigned.

You must previously define:

- skill types
- skills list
- skill levels

Tools are available that enable definition and display of the skills of team members.

Creating Controllers

To create a controller, you must create a person and associate the "Control Tester" profile.

*- For more information on creation of users and assignment of profiles, see the chapter "Managing Users" in the **HOPEX Power Supervisor** guide.*

Creating skill types

To create a skill type:

1. In the **HOPEX ORM** desktop, select **Administration > Skill Management > All Skill Types**.
2. Click **New**.
3. Enter a **Name** for the skill type, for example "Languages".
4. Click **OK**.

Creating skills

To create a skill:

1. In the **HOPEX ORM** desktop, select **Administration > Skill Management > All Skills**.
2. Click **New**.
3. Enter a **Name** for the skill, for example "English".
4. Click **OK**.

The new skill is added to the list of skills.

In properties of the skill you can indicate the **Skill Type** to which it is attached, for example "Languages".

Creating skill levels

You must now create skill levels to be associated with each skill type.

To create a skill level:

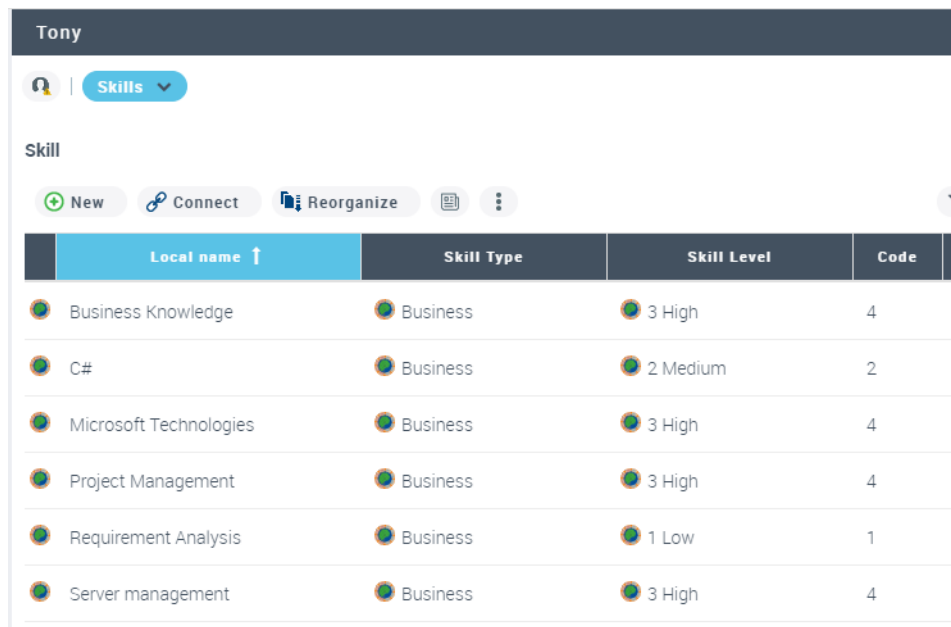
1. In the **HOPEX ORM** desktop, select **Administration > Skill Management > All Skill Types**.
2. Open the properties of the skill type that interests you.
3. In the **Skill Levels** section, click **New**.
4. Enter a **Name**, for example "Beginner".

5. Click **OK**.
6. In **Skill Level Value**, enter a figure corresponding to the skill level, for example "1" for "Beginner" (while "4" could correspond with "Experienced" in our example).
 - This figure gives a graphic view of the extent of controller skills in the test assignment page.

Defining skills for each user

To define the skills of a user:

1. In the **Administration** navigation pane, select **Skill Management > View Users With Skills**.
2. Select a user and click the **Person Properties** button.
3. In the properties, select the **Skills** page.
You can specify user skills as a function of previously defined skill types and skill levels.



Local name ↑	Skill Type	Skill Level	Code
Business Knowledge	Business	3 High	4
C#	Business	2 Medium	2
Microsoft Technologies	Business	3 High	4
Project Management	Business	3 High	4
Requirement Analysis	Business	1 Low	1
Server management	Business	3 High	4

Example of skills

Viewing skills

To view the skills and skill levels available within the team:

1. In the **HOPEX IRM** desktop, select **Administration > Skill Management > Manage Skills with Users**.

A list appears. You can sort the list by skill, skill level and user by clicking the header of the corresponding column.

View Users With Skills			
	Skill	Skill Level	Person (System) ▲
📁	Accounting	1 Low	Chandler
📁	Sales	3 High	Chandler
📁	English	3 Fluent	Chandler
📁	Sales	3 High	Ernesto
📁	English	3 Fluent	Ernesto
📁	French	2 Read/Written/Spoken	Ernesto
📁	Accounting	3 High	Ernesto
📁	Sales	2 Medium	Kim
📁	English	3 Fluent	Kim
📁	Accounting	2 Medium	Kim
📁	Sales	3 High	Luca
📁	Accounting	3 High	Luca
📁	English	3 Fluent	Luca

Managing Currencies

Currencies are used in the framework of tests for completion of expense sheets.

Two currency types should be distinguished:

- central currency
 -) *Central currency is the currency adopted as reference currency.*
- local currency
 -) *A local currency is defined for each user. By default it is the same as central currency.*

Defining Central Currency

-) *Central currency is the currency adopted as reference currency.*

To define central currency:

1. In the Administration application (administration.exe), login to the environment of interest to you.
2. Right-click the repository and select **Options > Modify**. The repository options window opens.
3. Select the **Installation > Currency** folder. The list of currencies available as standard appears on the right.
4. In the **Monetary Symbol** field, specify the symbol of your consolidation currency, for example "\$".
5. In the **Central Currency** field, select your consolidation currency, for example "US Dollar".
6. Click **OK**.
7. Exit the Administration application.

Defining Local Currency

You can choose a local currency different from the central currency. To do this, you must connect to **HOPEX Windows Front-End** with your login.

) *A local currency is defined for each user. By default it is the same as central currency.*

To modify user local currency:

1. Start **HOPEX Windows Front-End** and connect with your login.
2. In the desktop, select **Tools > Currency** and select the currency that interests you.
3. Exit **HOPEX**, dispatching your private workspace.

When you reconnect to **Web Front-End** with your login, the currency proposed by default for your expense sheet expenses is the currency you have just defined.

Modifying User Local Currency

) *A local currency is defined for each user. By default it is the same as central currency.*

Local currencies proposed to users of the application are defined with the **HOPEX Administration** application.

To define the list of local currencies:

1. In the folder where **HOPEX** is installed, launch "Administration.exe" and connect with a user that has data administration authorization rights.
2. Select the environment then the repository on which you want to work.
3. Right-click the repository and select **Options**.
The repository options window opens.
4. Select the **Installation > Currency** folder.
The list of currencies available as standard appears on the right.
5. Then select all the currencies that will be used locally by your users.
6. Click **OK**.
7. Exit the Administration application.

Managing Exchange Rates

To enter an exchange rate:

1. In the **HOPEX IRM** desktop, select **Administration > Tools > Exchange Rate**.
2. Click **New**.
3. In the window that appears, enter:
 - the **Currency Code To**.
 - the **Rate** of the source currency related to the final currency.
 - the **Rate Date Begin**.
 - *Several exchange rate periods can be entered for the same currency. When entering expenses, the most recent exchange rate is taken into account.*
 - *You must enter the exchange rate in both directions, for example:*
 - EUR->USD
 - USD->EUR

To view an exchange rate:

1. In the drop-down lists above the table, select the source and final currencies.
2. Click **Refresh**.
The exchange rates for the selected currency appear.

- To reverse the exchange rate, click button



Configuring Time Sheets

Time sheets are used in the context of audits/tests.

The functional administrator can configure time sheet default options.

The functional administrator can define:

- number of hours worked per day
- days not worked in enterprise

To configure this data:

1. From the main menu, select **Settings > Options**.
2. In the window that appears, expand the folders **Installation > User Management**.
3. In the right pane of the window, specify:
 - the number of **Hours/Day** for each auditor.
 - Default value is "8".
 - days corresponding to weekend
 - Default values are "Saturday" and "Sunday".

Managing Campaign Calendars

Assessment campaigns are based on calendars divided into calendar periods.

) A campaign calendar enables planning of campaigns and their division into periods called calendar periods. Campaign calendars can also be used in reports or to plan audits or tests.

A calendar often covers a period of one year, either a fiscal year or a calendar year. In the latter case, a calendar period can correspond to a quarter.

Creating Calendars

To create a calendar:

1. In the navigation menu, select **Test > Preparation > Calendars**.
2. In the right pane of the window, click **New**.
3. Enter the **Name** of the calendar and its begin and end dates.
4. Click **OK**.

You can then define calendar periods.

Creating Calendar Periods

To create calendar periods:

1. Open the **Properties** of the calendar.
2. Click the **Characteristics** tab.
3. In the **Calendar Period** section, click **New**.
4. Enter the **Name** of the calendar period and its begin and end dates.
5. Click **OK**.
6. Create other calendar periods in the same way.

The calendar is created. It can then be connected to a test plan.

Connecting a Calendar to a Test Plan

To connect a calendar to a test plan:

1. In the navigation menu, select **Test > Preparation > Plans**.
2. Open the properties of the test plan that interests you.
3. Click **Characteristics**.
4. In the **Calendar** field, click the arrow and select **List** to display the list of calendars.
5. Select the calendar to be connected to the test plan.
6. Click **OK**.

PREPARING TESTS

Functionalities described here essentially concern the GRC manager.

The lead controller intervenes to define the work program, which enables:

- execution of test activities
- assessment of controls by means of questionnaires

Preparation of tests consists of creating a test plan and tests, and planning these before controllers intervene in the field.

To prepare tests:

- > In the **HOPEX IRM** desktop, select **Testing > Preparation**.

Creating a Test Plan

The test plan is prepared by the internal control director.

The plan is generally defined on a period of one year. This plan contains all tests to be executed in the year.

) *The test plan is a description of the expected scope and conduct of the audit. It is carried out in accordance with auditing standards and practices. It comprises a description of the audit approach and the planning schedule. It comprises several tests carried out during a given period.*

To create a plan:

1. In the **HOPEX IRM** desktop, select **Test > Preparation > Calendars**.
2. Right-click the **Plan** folder and select **New > Plan**.
The new plan appears.
3. Open the properties of the plan.
4. In the **Characteristics** tab, modify the **Name** of the plan.
5. Select the **Nature** of the plan:
 - Audit
 - Test
 - Compliance
 - Mixed
 - If you have only the **HOPEX Internal Control** solution, the plan nature is automatically specified and cannot be modified.
 - Depending on the selected nature, a **Tests** and/or **Audits** tab appears in the properties of the plan.
 - If you selected "Test" or "Mixed" values, an assessment campaign is created at validation of the plan. This will enable generation of questionnaires to internal controllers for assessment of controls. For more details, see [Assessing controls](#).
6. Select the **Calendar** of the plan.
7. Modify the **Begin Date** and the **End Date** if necessary.
 - The **Status** is defined automatically by the workflow.
8. Click **Save**.

The plan is created.

You can now create tests directly in the plan page.

Planning Tests

Test planning is carried out by the GRC Manager.

) *A test is assigned to a controller in the framework of a plan.*

Creating a test

To create a test:

1. Click **Testing > Preparation > Plans**.
2. Open the properties of the plan that will include the test to be created.
3. Select **Tests** in the drop-down menu at the top of the page.
4. Click **New**.

The new test appears under the plan.

- *To define characteristics of the test, see [Defining test properties](#).*

Accessing tests

To access tests of a test plan:

- > Click **Testing > Plans** and expand a plan.
The tests (or audits, depending on the plan nature selected) corresponding to the plan appear.
 - *You can also access the list of tests via the menu **Test > Preparation > Tests**.*

Defining test properties

You can specify certain information on tests.

General characteristics

General characteristics of the test are:

- **Name**: test name.
- **Code**: you can assign a code to the test.
- **Included in the Initial Plan**: this attribute is defined automatically according to plan status at the time of creation of the test. It indicates if the test was present at plan creation, or if it was added later.
- **Entity** controlled
- **Lead Controller**: lead controller name.
- **Main Control Correspondent**
- **Objective** of the test.
- **Category** of the test:
 - "Compliance"
 - "Efficiency"
- **Status** of the test: this attribute is defined automatically and modified at workflow transitions.

Justification and workload

In this section you can enter the following characteristics:

- **Justification** of the test
- **Origin**: follow-up, specific, recurrent, etc.
- **Priority**: priorities can be specified for tests. You can select tests to be integrated in the plan based on this priority criterion.
- **Estimated Duration** (days).
- **Estimated Number of Resources**
- **Estimated Workload**
 - *The following characteristics are automatically calculated:*
 - **Effective Workload (Hours)**: calculated from the effective workload defined on time sheets or on activities if no time sheet has been entered.
 - **Estimated Number of Resources**

Scope?

You can connect business or organizational processes to the test.

These can be used to automatically generate the test work program.

- *For more details, see [Completing the work program manually](#).*

Milestones

In the **Milestones** section, you can indicate a **Planned Begin Date** and a **Planned End Date**. These dates constitute audit milestones.

- *You can choose to enter milestones at a later stage.*

Users

In the **Users** section, you can specify test participants:

- **Test Controller**: controllers having been previously defined, you can connect but not create controllers. See [Assigning resources to tests](#).
- **Person tested**
- **Other Participant in Test** (for information only)

Skills

You can specify skills required by controllers to execute tests.

To define skills required for the test:

- › In the **Skills** frame, click **New** or **Connect** to create a skill or connect an existing skill.

When assigning controllers to a test, you will be able to compare skills of controllers with skills required for the test. For more details on the report providing this information, see [Assigning resources to tests](#).

Summary

In **Summary** of the completed test, you can indicate:

- **Key Strengths**
- **Key Weaknesses**
- **Evaluation**: good overall level, can be improved, etc.

Creating "template" tests

"Template" tests are work programs specially prepared to be applied to new tests.

This status is exclusively reserved for tests of a plan which is itself defined as a template. It applies automatically to existing tests of the template plan, and is proposed at creation of a new test on this same plan.

To define a test plan as a template:

1. Click **Test > Preparation > Plans**.
The list of plans appears in the edit window.
2. Click the icon of the plan in question and select **To Be Validated > Set As Template**.

Selecting tests to be executed

HOPEX Internal Control provides decisional help in selecting tests to be executed.


You can sort tests according to certain criteria, in order to:

- view previous tests
- find tests planned but not finally executed

Viewing the test coverage report

HOPEX Internal Control supplies a report providing information on the number of tests executed on each entity between two dates. It indicates entities that require testing, and enables generation of the corresponding tests.

To access this report:

1. Click **Test > Preparation > Entity Coverage**.
2. In the edit window, select a begin date and end date.
3. If required, select the score obtained by the test or its status.
4. Refresh the report by clicking the Refresh button  at the bottom of the report.

For each tested entity the report presents:

- the **Number of tests** executed between the two dates (effective begin and end dates)
- the name of the last **Test**.
- the **End date** of the last test (effective end date), or its state if it is still in progress
- the **Score** of the last test.

To generate tests corresponding to one or several entities:

- › Select the entity or entities that interest you and click the **Generate Tests** button.
A wizard asks you to choose a target plan. The tests are generated.

Consulting test histories

Consulting the history of tests can simplify your choice of tests to be executed.

In the list of tests, you can consult assessments of the test. You can sort tests based on this criterion, allowing you to create tests on appropriate entities.

To group tests by assessment:

1. Select **Test > Preparation** then **Tests**.
2. Click the "Evaluation" column title.
Tests are then sorted by this criterion.
An arrow associated with the column enables ascending or descending sort order.

Consulting tests not executed

Tests can remain in "Published" status never to be executed, due to another test being of higher priority.

Tests published or in progress can also be canceled via the workflow.

Grouping tests by status enables identification of those that must be recreated on a subject.

To find tests not executed of a previous test plan:

1. In the navigation menu, select **Test > Preparation > Tests**.

2. In the list of tests, click the title of the "Status" column.
 - *If the column does not appear, you can display it using the arrow located at extreme right of a column header.*

Tests are then sorted by this criterion.

An arrow associated with the column enables ascending or descending sort order.

Test assessment and status are defined in its properties. For more details, see [Defining test properties](#).

Viewing previous test expenses

A report allows you to view expenses of previous audits.

To access this report:

1. Click **Test > Preparation > Plans**.
2. Select a **Plan** and open its properties.
3. In the drop-down list, select **Plan Reports > Expenses**.

You can view expenses:

- By category
- By resource (auditor, controller or tester)

Selecting tests to be integrated in the test plan

Tests become active after validation only. Among all tests, some are part of the definitive plan, while others are discarded.

HOPEX Internal Control proposes tools simplifying selection of tests to be integrated in the plan.

Discarding tests

Potential tests considered of low priority can be discarded via the workflow.

To discard a test:

1. Click **Test > Preparation > Potential Tests**.
2. Click the icon of the test to be discarded and select **To Be Validated > Discard**.

The test is discarded but not deleted. It could serve as a template for a new test the following year.

Validating tests

You can validate tests:

- globally, at validation of the test plan
- individually

Planning tests using a Gantt chart

A report allows the internal control director (or GRC manager) to plan the different tests of a test plan.

To display this report:

1. Under **Testing > Plans**, select the plan in question.
The plan properties appear in the edit area.
2. In the drop-down list of the property page, select **Schedule**.
A Gantt chart describes tests of the plan.

By default, planning relates to the current year, but you can view audits over a more precise period.

You can redefine the Gantt chart display period:

- by selecting a calendar period.
- or specific begin and end dates.

You can modify test dates in the diagram:

- by moving the period begin or end dates using the mouse.
- by clicking the center of the period and by moving the mouse to simultaneously move the begin and end dates.

Zoom functions allow you to customize display (zoom in and out in the calendar).


You can add tests from this chart.

Assigning resources to tests

Before assigning a resource to a test, you can view its availability and skills.

Viewing resource availability

To view resources available with necessary skills for a test:

1. Open the properties of the test plan concerned.
2. In the drop-down list select **Plan Reports > Resource Allocation**.
By default, the report presents tests of the test plan over the year. You can display those of a particular period.
3. In the table at top left, select a test.
4. In the table at top right, select a resource of which you wish to display availability.
 - *You can select several resources.*
5. In the lower frame "Assign Resources", click the **Refresh** button .

Two charts present:

- Skills required by the test and skills of the selected resource.
 - Availability of the resource on test dates.
The color of the test period depends on the number of resources assigned to it related to the estimated number of resources:
 - Green if the test has a sufficient number of resources
 - Orange if resources are insufficient
 - Red if no resources are assigned
- *These two charts should be refreshed separately.*

Assigning a resource to a test

To assign a resource to a test:

1. In the **Assign Resources** page of the test plan properties, in the top left frame, select the required test.
2. In the frame at top right, select a person.
3. Click the **Assign** button.
 - To remove a controller from the test, carry out the same procedure, but click the **Unassign** button.

Specifying a lead controller for a given test

To specify the lead controller on a test:

1. Open the properties of the test concerned.
2. Specify the **Lead Controller** field.

Sending the Notification Letter

After having completed the specifications required for execution of a test, the internal control director can send a notification letter informing controlled persons of the test.

Sending this notification letter is not included in the workflow. It precedes the next step in the workflow which consists of publishing the test.

Creating notification letters

To create the test notification letter:

- > Click the icon of the test and select **Deliverables > Notification Letter**. A message asks if you want to open or save the file. The document presents the comment entered in characteristics of the test.

When the document has been saved, you can open and modify it.

You can also connect it to the test as a business document, under the "notification letters" category.

Connecting the notification letter to the test

The file is generated from test content, but is not connected by default to the test.

To connect the notification letter to the test and make it a business document:

1. Open properties of the test.
2. In the drop-down list, select the **Documents** page.
3. Click the **New** button.
The **Creation of Business Document** dialog box appears.
4. Indicate the business document name.
5. In **File Location**, click the **Browse** button.
The **File Location** dialog box appears.
6. Click **Browse** and select the file.
7. Click **Upload**.
8. In the document creation dialog box, in **Document Pattern**, select "Notification Letter".

9. Click **OK**.
The document appears in the list of documents attached to the test.

Validating tests

When the internal control director decides that a test should be executed as part of the test plan, he/she validates the test.

- *An assessment session is created. This will enable generation of questionnaires to internal controllers for assessment of controls. For more details, see [Assessing controls](#).*

Publishing tests

HOPEX Internal Control enables preparation of tests and only making these public to controllers when planning is completed.

To make a test public:

1. Right-click the icon of the test.
2. Select **To Be Published** > **Publish**.

Test status changes to "Published".

Having been published, tests appear in the work program of controllers.

Preparing Tests

Supervision of test progress is assured by the lead controller. In the test preparation phase, he/she establishes the work program and assigns activities to controllers.

Work program creation prerequisites

So that the work program can be generated:

- processes (organizational or business) must be connected to the entity
- controls must be connected to processes

Work program content

HOPEX Internal Control enables automatic creation of a work program structure from:

- the tree of processes connected to the entity, or
- the processes specified in the test scope
 - *If no process has been specified in the test scope, all processes connected to the entity will appear in the work program.*

Environment objects	Objects created in the work program
Process (organizational or business)	Test theme
Control (connected to process)	Test activity

- *The entity is represented by the test.*

Test theme

A theme corresponds to a process.

Themes can be used to group test activities and workpapers, that is to organize test content.

Test activity

A test activity corresponds to a control.

It is the basic element of the test. It enables assignment of responsibility to the controller.

Workpaper

A workpaper comprises points to be checked on a given subject in the course of an audit activity.

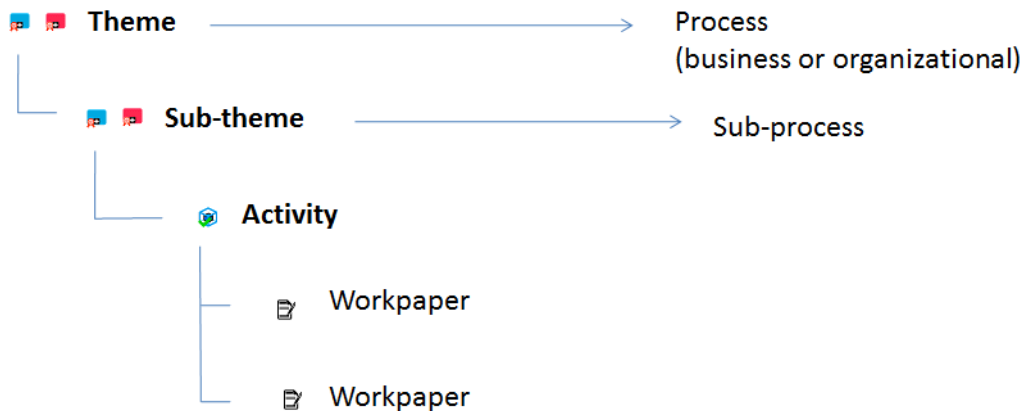
A workpaper is generated for each generated test activity. For more details, see [Creating workpapers](#).

Creating work programs automatically

To create a work program automatically:

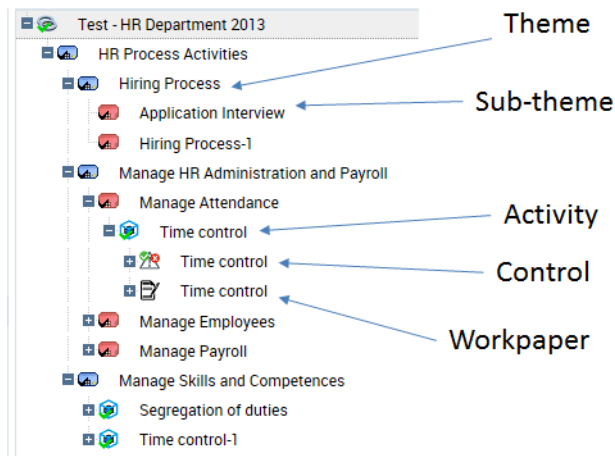
- > Click the icon of the test and select **Generate Work Program**. This command will duplicate the tree of processes for the entity in the scope of the test.

If processes are explicitly specified in the test scope, only these processes will be automatically generated in the work program structure.



Completing the work program manually

The lead controller can complete the test manually to specify its content. He/she can add or remove themes/activities in the **Work Program** tab of the test.



Creating themes

To create a theme:

1. In the properties of a test, select the **Work Program** page.
2. Click the icon of the test and select **New > Test Theme**.
The theme created appears in the tree of the work program.

3. Display properties of the theme.
You can:
 - modify its name
 - select a parent test theme (if you want to create a tree of themes)
 - connect the test theme to a process
 - enter a comment
4. Click **OK**.
You can view the tree of themes and sub-themes created. You can now create activities and workpapers.

Creating activities

A test activity is a test element relating to a control.

To create an activity:

1. In the properties of a test, select the **Work Program** page.
2. Click the icon of the test (or theme) and select **New > Test Activity**.
The activity created appears in the tree of the work program.
3. Display properties of the activity.
4. Enter the name of the activity.
5. Connect the activity to a **Theme** if you want the activity to be located under a theme in the tree.
6. Connect the test activity to a control.
7. Select the **Owner** of the test activity, who can be a controller or the lead controller of the current test.
8. Indicate the **Estimated Workload**.
 - *You can later manually enter the effective workload on this activity.*
9. Click **OK**.

Assigning activities

For each activity, the lead controller specifies:

- Start and end dates
- Estimated workload
- Controller responsible for execution

To enter this data:

1. In the properties of the test, select the **Activities** page.
2. Open the properties of the test activity concerned.
3. In the **Test Activity Owner** field, using the right-pointing arrow, select a controller from among the candidate controllers.
4. Enter test activity start and end dates.
5. Specify the workload.

Reviewing the Work Program

The lead controller can proceed with a report on the work program. This report enables a check that:

- task assignment has been correctly carried out
- the work program covers the appropriate risks and processes

Consulting the work program report

To access work program reports:

- > In the page of a test, select **Reports > Work Program**.

You can view:

- comparison of resources allocated and resources available:
- workload (in person/days)
- workload by theme (in person/days)
- activities by theme

Exporting the workload under Excel

The work program under Excel covers themes, sub-themes, activities and workpapers.

Having the work program available under Excel allows:

- consultation of the complete work program without having to access objects individually
- storage of a printed version of the work program
- viewing tasks to be executed at indication of an issue

To export the work program:

- > In the **Work program** page of the test, right-click the tree root and select **Deliverables > Export Work Program (Excel)**.
 - *A pop-up window opens at the bottom of the page. If your navigator blocks these windows, you cannot see file export. In this case, deactivate pop-up blocking in the navigator.*

You can then modify the work program in Excel.

When the work program has been modified, you must create a business document in **HOPEX Internal Control** and reimport the modified work program.

To create the business document corresponding to the modified work program:

1. In the properties of the test, select the **Documents** page.
2. Click the **New** button.
3. Enter the name given to your work program.
4. Select the location where you stored the modified Excel file and click **Upload**.
5. Select the "Work Program" document template.
6. Click **OK**.

The modified work program is now stored in the **HOPEX** repository.

Validating work programs

When the lead controller validates the work program via the workflow, an assessment session is automatically created and connected to the test. Assessment questionnaires are generated and made available from test activities. Respondents are owners of test activities.

- *For more details, see [Assessing controls](#).*

To validate the work program:

- > Click the icon of the test and select **To Be Validated > Validate**.

Executing administrative tasks

Planning resources

Auditors/controllers can be assigned to different audits/tests at the same time. It is therefore important to enter the time allocated for each auditor to an audit.

To indicate for each auditor/controller the time to be allocated to an audit/test:

1. In the properties of the audit, expand the **Users** section.
2. Select a user and in the **Workload (Hours)**, enter the time to be spent on the audit/test.

Creating general tasks

For controllers, the director can create tasks not directly linked to tests.

To create a general task:

1. Select **Testing > Preparation > General Tasks**.
2. Specify dates and a comment and connect users to this task.
Users assigned to this task can allocate hours to this task in their time sheet.

Validating Vacations

To display vacations in auditor time sheets, you must previously have validated the vacation.

To validate the vacation:

1. Select **Test > Preparation > Vacation Requests** and open the properties of the vacation to be validated.
2. Position its status as "Validated".

Initializing expense sheets

The lead auditor can create an expense sheet per auditor/controller for all auditors/controllers assigned to the audit/test. In this case it consists of initializing expense sheets.

To initialize expense sheets:

1. In the audit/test properties window, select the **Expenses** page.
2. Click the **Initialize** button.
An expense sheet is created for each auditor/controller.

To create an expense:

1. In the expense sheet properties, expand the **Expenses** section and click **New**.
2. Enter for each expense:
 - an **Amount**
 - a **Date**
 - the **Expense Category**: "Lodging", "Food and Beverages", "Transportation"
 - a **Comment** if required.

- The auditor enters the amount in the desired currency. The converted amount is calculated automatically.

EXECUTING TESTS

- Procedures described here apply to the "Internal Controller" profile only.

Preparation of a test work program allows internal controllers to:

- execute tests on samples using test sheets.
 - These test sheets are presented in the form of check-lists. Questions are asked for each object present in the constituted sample.
- assess controls in terms of design and efficiency by means of questionnaires.
 - These are the same questionnaires as those covered in the chapter concerning assessment campaigns.

Consulting the Work Program

The controller needs to consult:

- his/her work program.
- the global work program, for a clearer view of tasks to be executed.

To access your work program:

- > From the navigation menu, click **Test > Preparation > Work Programs**.
 - To print the work program you can export it under Excel. For more details, see [Exporting the workload under Excel](#).

Executing Tests on Samples

Internal controllers execute the test steps defined on controls on samples.

To be able to complete test sheets, you must first:

- generate or create workpapers
- specify or modify test sample size
- generate the test sample
- define test sheet questions

Creating workpapers

Workpapers are folders or work documents that serve as a basis for the controller in execution of the test.

- Workpapers are created automatically at generation of the work program. For more details, see [Work program content](#).

To create a workpaper manually:

1. In the properties of a test, select the **Work Program** tab.
2. Select the activity concerned and display its properties.

3. In the **Characteristics** page of the activity, **Workpapers** section, click the **New** button.
The workpaper appears:
 - in the test activity page
 - in the tree of the test work program
4. In the work program, select the paper to display its **Properties**.
5. Enter a name and your comments.
6. Click **OK**.

Specifying or modifying the sample size

The controller must specify the size of the test sample on the workpaper. This is the number of elements to be tested.

To specify sample size:

1. In the properties of a test, select the **Work Program** page.
2. From the work program, open the properties of a workpaper.
3. Specify the **Sample Size**.

This is the size of the sample selected for testing.

- By default, the value is inherited from the sample size specified on the control. For more details, see [Defining Test Sheet Questions](#).

Generating the test sample

Test samples are generated directly from information available on the control (test steps).

To generate samples:

1. In the properties of a test, select the **Work Program** page.
2. From the work program tree, click the icon of a workpaper and select **Generate Test Sample**.

Depending on the previously specified sample size, a message informs you of the number of elements that will be created in the test sample.

Generated test samples are available in the properties of the workpaper

Defining test sheet questions

Workpapers contain test sheets, which represent in tabular form the points to be executed. These test sheets contain:

- in rows, the elements of the sample to be controlled
- in columns, the questions (represented by test steps)

You must define check-list questions before being able to generate test sheets.

- For more details, see [Preparing Control Testing](#).

Completing the generated test sheets

To be able to view test sheets, you must first:

- define test sheet questions
 - See [Defining Test Sheet Questions](#).
- generate the test sample
 - See [Generating the test sample](#).

To view the test sheet:

1. In the properties of a test, select the **Work Program** page.
2. Open the properties the question that interests you.
3. Select the **Test Sheet** tab.

This test sheet presents:

- in rows, the elements of the test sheet to be controlled
- in columns, the test steps

You can reply to the questions in the columns provided.

- *Test sheet questionnaires are distinguished from assessment questionnaires. For more details on assessment questionnaires, see [Assessing controls](#).*

Assessing test activities

After specifying test sheets, the controller can globally assess the test activity and therefore specify test results.

- *This "expert view" assessment can be based on results of test sheets, or not.*

To assess the test activity:

1. Open the properties of the test activity.
2. In the **Test Result** field, specify if the test has:
 - Failed
 - Passed
 - Not yet been assessed

Assessing Controls

Internal controllers must assess controls in terms of design and efficiency.

- *This assessment uses standard assessment campaign mechanics. Generated questionnaires are distinguished from those corresponding to test sheets.*

Generating questionnaires

The questionnaires are generated at validation of the work program.

- *For more details, see [Validating work programs](#).*

Responding to Questionnaires

You can answer control assessment questionnaires:

- on a test
- on each activity of a test

To view test questionnaires:

1. From the navigation menu, click **Test > Preparation > Tests**.
2. In the properties of the test, expand the **Assessment** section.
3. Select a questionnaire and click **Display Questionnaires**.
4. Select the questions and reply to these in the lower part of the window.
5. Click **Save**.

To view test activity questionnaires:

1. In the properties of a test, select the **Work Program** page.
2. In the pop-up menu of a test activity, select **Assessment**.

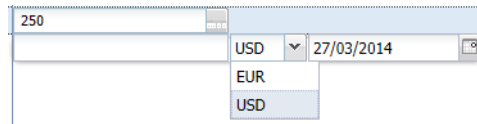
Managing Time and Expenses

Managing expenses

Auditors/controllers assigned to an audit/test can create expense sheets on this audit /test. In this case, they must submit their expense sheet to the lead auditor via a workflow.

To create an expense sheet:

1. In the **HOPEX IRM** navigation menu, select **My tasks > Test > My Expenses**.
2. Click **New**.
3. In the **Expense Owner** field, select the audit/test concerned.
 - You can also create an expense sheet in the **Expenses** page of the audit/test properties. In this case, you do not need to specify the expense owner.
4. Click **OK**.
An expense sheet is created. You can now create associated expenses.
5. In the **Expenses** section of the expense sheet, click **New**.
6. In the properties of the expense sheet, enter an **Amount** and a **Date**: you can enter the amount in the currency you require (from those you can access).



The screenshot shows a form with a text input field containing the number '250'. To the right of this field is a dropdown menu for currency selection. The dropdown is currently open, showing three options: 'USD', 'EUR', and 'USD'. The first 'USD' option is selected. To the right of the dropdown is a date input field containing '27/03/2014'.

- The amount is converted to the currency configured for your user.

7. Specify if required:
 - the **Expense Category**: "Lodging", "Food and Beverages", "Transportation"
 - a **Comment**.

8. Click the icon of the expense sheet and submit it via the workflow.
 - *The lead auditor does not need to seek approval for his/her expense sheets.*
 - *You can export to Excel the data contained in expense sheets.*

Entering vacations

Entering vacations enables to:

- improved planning of test campaigns.
- pre-filling time sheets.

To enter a vacation:

1. In the **HOPEX IRM** navigation menu, select **My tasks > Test > My Vacation Requests**.
2. Click **New**.
3. In the properties, select the associated **Plan**.
4. Also specify:
 - **Vacation Type** (holiday, training, other)
 - planned and effective begin and end dates
 - a comment if required
5. In the **Status** field, select "Submitted".
 - *So that the vacation will appear in the time sheet, the lead controller must have validated the vacation (by positioning its status value on "Validated").*
 - *An auditor/controller can modify or delete a vacation as long as the vacation has not been validated.*

Completing a Time Sheet

Auditors/controllers can complete time sheets in the framework of their audit/test.

To complete a time sheet:

1. In the **HOPEX IRM** navigation menu, select **My tasks > Test > My TimeSheets**.
The time sheet displays one line per audit/test.
2. Enter for each day the number of hours spent on each audit/test.
3. Click **Submit** to save your time sheet.
4. Click **Next** to enter your hours concerning the next week.
 - *Messages may appear if the activity report is not consistent. For example, if hours have been allocated to an audit/test and the audit/test has not yet started. You can submit an incomplete time sheet.*

The time sheet enables entry for each day and for each week the number of hours spent on each audit/test.

- *Only those audits/tests that have been published are visible in the time sheet.*

The time sheet also shows:

- vacations that have been validated
- general tasks (meetings, training, team management, administration ...)

Management of issues and action plans

The controller completes the work program by entering:

- Issues
- Action Plans

Managing issues

Creating Issues

Issues are accessible from test activities.

To create an issue:

1. In the **HOPEX IRM** navigation menu, select **My tasks > Test > Activities to Perform**.
2. Click the icon of the activity concerned and select **New > Issue**.
The issue appears in the work program tree as well as in the properties of the activity.

Saving test evidence

You can connect documents to illustrate an issue.

To add a document as an attachment:

1. In the tree of the work program of a test, select an issue to which you wish to add a document.
2. Expand the **Attachments** section.
3. Click **New**.

The business document creation window opens.

) A business document is a document whose content is independent of the repository. This document can be MS Word, MS Powerpoint, or other files. A report (MS Word) generated on an object can become a business document.

4. Indicate the business document name.
5. In **File Location**, click the **Browse** button.
The **File Location** dialog box appears.
6. Click **Browse** and select the file.
7. Click **Upload**.
8. Click **OK**.

The document appears in the list of documents attached to the issue. It is owned by the test of the issue. You can therefore also see it appear in the **Documents** tab of the test.

Managing action plans

Action plans can be created from issues.

To create an action plan:

- > In the properties page of an issue, expand the **Action Plans** section and click **New**.
The action plan appears in the section.

To define properties of the action plan:

1. Select the action plan and click **Property**.
2. Modify its **Name** if required.
3. Select a level of **Priority**.
4. Specify the **Means** implemented for the action plan.
5. Modify the **Owner** if required.
 - *By default the owner is the action plan creator.*
6. Select an **Approver**.
 - *By default the approver is the action plan creator.*
7. Click **OK**.

Supervising Tests

The lead controller must validate the work of controllers via the activity workflow.

He/she can then check their work and assure test follow-up. To simplify the task, reports enabling test check are available on each test.

Test check reports

To access test check reports:

- > In the properties of a test, select the **Reports > Supervision** page.

Three reports appear:

- **Issue Objectivity**: to ensure objectivity of issues, evidence must be provided.
The figure displayed represents the percentage of issues with at least one attachment.
- **Work progression by controller**
- Controller activity **Summary Table**

Time sheet follow-up reports

Reports enable follow-up of auditor/controller time sheets.

- *These reports are available for Compliance Managers only.*

To access the Reports tab:

- > In the navigation menu, select **Test > Follow-up > TimeSheet Reports**.

Three reports are available from a drop-down list.

Time sheets by auditor

This report presents auditor time sheets over a given period

- number of hours assigned for the audit
- effective number of hours in week
- number of hours accumulated since start of audit
- number of hours remaining
- last allocation of auditor on audit
- last time sheet of the auditor
- progress of auditor on audit (in progress, completed..)

Time sheets by audit

This report presents all time sheets for a given audit.

Incomplete days by auditor

This report presents the list of incomplete days, that is days of which the number of hours declared is less than daily work duration.

- Press **Validate** to validate the Time Sheet.

Test expenses reports

To view expenses of an audit/test:

- > In the properties of a test, select the **Reports > Work Mission Expenses** page.

Pie diagrams present breakdown of expenses:

- by resource (auditor)
- by category:
 - Food and Beverages
 - Lodging
 - Transportation

To view the list of expenses associated with a diagram sector:

- > Right-click in a sector.
Corresponding results appear as a list in the lower part of the window.

Concluding Tests

Test assessment reports

Reports allow the lead controller to best assess the test and analyze its action plans.

To access the Reports tab:

- > In the properties of a test, select the **Reports > Assessment** page.

Several reports are proposed:

- Action plan breakdown by priority (low, medium, high)
- Issues by theme
- Summary table of above elements

Generating test reports

The test report uses test elements.

To generate the test report:

1. In the properties of a test, select the **Work Program** page.
2. Click the icon of the test and select **Deliverables > Test Report**.
A message asks if you want to open or save the file.
3. Save the file to be able to modify and then submit it.

Assessing tests

To assess the test:

1. In the **Characteristics** page of the test properties, select the **Summary** section.
2. You can indicate:
 - Test **Key Strengths**
 - Test **Key Weaknesses**
3. In the **Assessment** field, specify a value from:
 - "Good overall level"
 - "Can be improved"
 - "Improvement needed"
 - "At risk"

Terminating tests

When the test is closed:

- the test report is sent to persons interviewed
- action plans are sent to their owner

Closing tests

When the test has been terminated, the internal control director can close it.

- *Closing a test closes all objects at a lower level, with the exception of action plans and actions. When these objects have been closed you can no longer modify them.*
- *The administrator can exceptionally reopen these objects if necessary.*

TEST FOLLOW-UP

Implementing Action Plans

Accessing action plans

To access action plans:

- > In the navigation menu, select **My Tasks > Action Plans/Recommendations > Action Plans to Implement**.
This list presents the action plans assigned to you.

Implementing actions

The action plan owner must create actions.

Creating actions

To create an action:

1. Open the properties of a test.
2. In the **Action Plans** tab, select an action plan and click **Properties**.
3. In the **Actions** section, click **New**.
4. Open the properties of the action created.
5. Modify its name if necessary, enter a date limit and an action owner.
6. Click **OK**.

Sending or submitting the action plan

Actions created and assigned to appropriate users constitute an action plan.

To submit the action plan:

- > Right-click the action plan name and select **To Be Sent > Send**.

The approver validates the action plan by return.

- *By default, the approver is the controller who created the action plan.*

Action plan implementation follow-up

When the action plan has been validated by the approver, actions are implemented by persons concerned.

Specifying action plan progress

The action plan owner must inform the approver on progress of his/her actions.

To indicate progress of an action plan:

1. In the properties of an action plan, expand the **Progress Update** section.

2. Click the **New** button.
A progress state is created.
3. In the **Progress Update Percentage** field, specify an action plan execution percentage.
4. Enter a comment if required.
5. Click **OK**.

– Several progress states at different dates can be created.

Following up action plan progress

After a predetermined period, the internal control director or lead controller can request receipt of information on progress of action plans.

To follow up action plan progress:

- > In the action plan properties, select the **Progress Report** page.

Action Plan Follow-Up

An analysis report assures follow-up of action plans.

To access action plan follow-up reports:

- > In the **HOPEX IRM** desktop, select **Analysis > Action Plans > Follow-up**.

To create an action plan report:

1. Click **New** and open the report created.
2. In the **Parameters** page, connect the objects that interest you:
 - Processes
 - Entities
3. In the **Reports** page, you can view the distribution of action plans by:
 - status
 - progression
 - priority
 - category
 - nature
 - processes
 - entity

Test Plan Follow-Up

HOPEX Internal Control enables follow-up of test plans according to different criteria.

Displaying test plan follow-up reports

Reports enable test plan execution follow-up.

To access test plan reports:

1. Open the properties of the plan.
2. Select the **Plan Reports** page.

Supervision

This report offers a summary of test plan tests according to different criteria:

- Origin
- Priority
- Category
- Score
- Status

Workload and resources

This report enables comparison of estimated and effective workloads.

Pie charts show comparison of test design and efficiency.

Resources allocation

The diagram displayed in this report enables comparison of:

- persons available
- persons required
- persons assigned

By default, results relate to the current year, but you can display results for a precise period.

Gantt report

The Gantt report comprises two parts:

- A Gantt chart of plan tests scheduled between selected dates
- A Gantt chart of occupation of controllers on plan tests between selected dates

Expenses

This report shows all expenses linked to a plan, as well as breakdown by expense category and by controller.

It allows the director to plan future audits.

Closing a test plan

When all test activities have been completed, the internal control director can close the test plan.

The effect of this action is to close all tests in progress that have not been canceled.

Dashboard

Your dashboard allows you to access a set of widgets and follow the progress of your tests in real time.

To customize your dashboard:

1. From the navigation menu, select **Dashboard**.
2. Click **Add**.
The list of elements you can display in your dashboard appears:
 - general widgets
 - IRM-related widgets
3. Select an element.
It appears in your dashboard.



REPORTS RELATED TO CONTROLS



This chapter describes reports present in the **Analysis** navigation tab. This tab groups the main reports used in each step of internal control. They can provide help in decision-making and allow you to follow up progress of your work.

- You find these reports in navigation tabs corresponding to the different internal control phases. You can also find certain reports in the properties dialog boxes of the objects they describe.

- 6 [Control Library Reports](#)
- 6 [Control Execution Reports](#)
- 6 [Control Assessment Reports](#)
- 6 [Assessment Follow-Up Reports](#)
- 6 [Control Testing Reports](#)
- 6 [Issue Follow-up Reports](#)

CONTROL LIBRARY REPORTS

Control Identification

This report presents distribution of controls according to several perspectives:

- entities
- processes
- control types
- accounts

Access path

Analysis > Control > Identification > Control Location Matrix

Parameters

Parameters	Remarks
Begin Date	Optional All controls created after this date are selected
End date	Mandatory Initialized with current date All controls created before this date are selected
Context objects	Optional The context object can be an: <ul style="list-style-type: none"> - Entity - Control type - Process - Account

Connecting context objects

You can specify context objects enabling display of controls linked to:

- Entities
- Processes
- Types of control
- Accounts

To connect context objects:

- > In the appropriate frame, click **Connect**
In the dialog box that appears, you can select objects in two ways:
 - via a tree: select the objects to be connected in the proposed tree and click **OK**.
 - via the query tool: select the required object type in the drop-down list, click the **Find** button, select the objects to be connected and click **OK**.

Results

To obtain the list of controls making up a bar chart bar:

- > Click the bar chart bar that interests you.
The list of controls taken into account is presented at the bottom of the edit area.

Bars of the bar chart distinguish assessed controls from those not yet assessed.

Control Location Matrix

The control location matrix displays links between:

- a controls list
- context objects

Access path

Analysis > Control > Identification > Control Location Matrix

Parameters

Parameters	Parameter type	Comment
Begin Date	Date	Optional All controls created after this date are selected

Parameters	Parameter type	Comment
End date	Date	Optional All controls created before this date are selected
Context type	The context can be of type: - Account - Business process - Control type - Entity - Organizational process	Mandatory The object type determines contexts to be displayed in matrix columns
Localized controls	List of controls possibly filtered by: - Entity - Process - Risk type - Account	Mandatory Controls to be displayed in matrix rows

Control Map

The control map constitutes the control "identity card".

Generating the control map

To generate a control map:

- > In the **Control Library** navigation tab, click the icon of the control then the **Generate Report (MS Word)** button.

An MS Word format report opens.

- *An intermediate window may ask if you want to authorize pop-ups. If this is the case, reply "Yes".*

Control map content

For the control concerned, the control map presents:

- control characteristics
 - general characteristics
 - responsibilities (in the RACI sense)
 - scope (context objects)
- data concerning control execution
 - execution method (frequency, associated steering calendar, execution procedure, associated controls)
 - executions carried out (with respondent and date)

CONTROL EXECUTION REPORTS

- 6 [Detailed Execution Results](#)
- 6 [Consolidated Execution Results](#)
- 6 [Following Up Execution Sessions](#)

Detailed Execution Results

This report presents results of each execution campaign session.

Access path

Analysis > Control > Execution > Detailed Execution Results

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Result

The report is presented as a table:

- in rows: tree of controls in their context
- in columns: results (control level)
 - *This report is available only in the **Reports** navigation tab.*

Consolidated Execution Results

This report presents aggregated results of controls by entity and by month.

Access path

Analysis > Control > Execution > Consolidated Execution Results

Parameters

Parameters
calendar
Begin Date
End date
Entity type
Entity

Result

The matrix comprises:

- a list of entities: by default, all entities are selected.
 - If the "Entity type" parameter is specified, selected entities correspond to this specified entity type.
- a **Total number of controls**: number of controls linked to the entity (or its sub-entities).
- a **Total number of instances**: controls are counted as many times as there are contexts for the same control.

If a control is assessed in the framework of two different entities, the control is counted twice: **HOPEX Internal Control** distinguishes two instances of the assessed control.

- For more details on control contextualization see [Contextualizing Controls](#).

- for each month:
 - a **Number of assessed instances**
 - a number of instances considered as satisfactory ("pass")
 - a % of instances considered as satisfactory ("pass")

Following Up Execution Sessions

This report enables follow-up of assessment sessions of "Execution" type.

Access path

Analysis > Control > Execution > Execution Session Follow-Up

Availability

This report is also available from a particular execution session.

To access this report from an execution session:

1. In the properties of an execution campaign, select the **Sessions** tab and open the properties page of an assessment session.
2. Select the **Reporting** tab, then **Follow-Up**.

Parameters

Parameters
Session

Result

A summary displays general information on the current session.

This report presents charts concerning campaign progress:

- Percentage of completed questionnaires
- Distribution of questionnaires by status
- Distribution of questionnaires delegated/not delegated
- Distribution of questionnaires by status, for each respondent
- Distribution of questionnaires by status, for each assessed object

CONTROL ASSESSMENT REPORTS

Campaign Result Tree

This report presents results of a given execution campaign session. It presents entities/processes/controls as trees and indicates for each assessed control whether it is satisfactory or not.

Access path

Assessment > Results > Control Assessment Campaigns > Campaign Results Tree.

Parameters

Parameters
Campaign
Assessment session

Campaign Result Matrix By Entity

This report presents as a matrix the results of each session of a given assessment campaign.

Access path

Assessment > Results > Control Assessment Campaigns > Campaign Result Matrix by Entity.

Parameters

Parameters
Campaign
Entity
Entity type

Aggregation Report

The aggregation report presents in tree form all objects from the selected root entity, together with their last assessment.

Access path

Assessment > Results > Aggregation

Parameters

Parameters	Remarks
Begin Date	
End date	By default current date
Context root	Tree root entity
Aggregation schema	An aggregation schema should be selected from the proposed list
Assessed characteristics	Assessed characteristics proposed depend on the selected aggregation schema.

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

ASSESSMENT FOLLOW-UP REPORTS

Session Follow-Up

This report enables assessment session follow-up.

It is identical to the "Execution Sessions Follow-Up" report, except that it is started from an assessment session (the campaign not having "Execution" type).

- For more details, see [Following Up Execution Sessions](#).

Access path

Assessment > Results > Sessions > Session Follow-Up

Parameters

Parameters	Parameter value
Session	Assessment session

Session Statistics

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

Access path

Assessment > Results > Sessions > Session Statistics

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Result

A tree appears:

- in rows: questions/answers, together with respondents
- in columns: for each question/answer:
 - number of respondents
 - controls to which the answer relates

This tree specifies who has answered what to which question.

CONTROL TESTING REPORTS

Testing Coverage

The testing coverage report provides help in decision-making when selecting tests. It enables generation of tests.

- See [Viewing the test coverage report](#).

Plan Synthesis

This report presents an overview of plan indicators.

Access path

Analysis > Testing > Plan Synthesis

Result

A summary table presents:

- number of tests (total number, number of tests planned, published and completed)
 - *If you click the figure indicated, the corresponding tests appear at the bottom of the window. You can consult the properties of each test and modify these from this list.*
- estimated and effective workload (in days)
- average duration (days)
- average number of controllers

Charts present the distribution of tests by:

- origin
- priority
- category
- score
- status

Other Reports

Reports allow you to follow up progress of a particular object (test plan, test, action plan). They are available on each object, in the **Testing** navigation tab.

Test plan follow-up reports

Reports enable test plan execution follow-up.

- See [Displaying test plan follow-up reports](#).

Test follow-up report

For more information on possibilities for test follow-up in particular, see:

- [Planning tests using a Gantt chart](#)
- [Viewing resource availability](#)
- [Consulting the work program report](#)
- [Generating test reports](#)
- [Test expenses reports](#)
- [Supervising Tests](#)
- [Test assessment reports](#)

Action plan report

To follow up progress of an action plan in particular, see [Following up action plan progress](#).

ISSUE FOLLOW-UP REPORTS

The issue follow-up report is presented in the form of a pie chart.

Access path

Analysis > Controls > Remediation

Result

This report distinguishes issues:

- **Remediated:** issues with an action plan whose status is:
 - Completed
 - Closed
- **Non-Remediated:** issues with an action plan of which status is:
 - To send
 - To start
 - Under follow-up
- **Without action plan**
 - For more details on generation of this report, see [Generating issue follow-up reports](#).
-

MANAGING ISSUES AND ACTION PLANS



Issues are identified from control assessment questionnaires. Their analysis enables implementation of the appropriate corrective actions in the form of action plans. Action plan follow-up is simplified by production of reports.

- 6 [Managing issues](#)
- 6 [Managing Action Plans for Internal Control](#)

MANAGING ISSUES

Issues are created automatically at control assessment when controls are considered unsatisfactory. They can also be created manually.

Automatic Issue Creation

In the framework of a test activity, if an activity is the subject of a poor assessment, an issue is automatically proposed to the questionnaire respondent.

The issue is connected to:

- the questionnaire concerned
- the assessed control
- the measurement of the control concerned

To view the origin of the issue:

1. In the **HOPEX IRM** desktop, select **Test > Remediation > Issues**.
2. Select the issue created automatically and expand the **Assessment Scope** section.

This section provides information on the origin of the issue:

- questionnaire
- source measure: the control and its context object (process or entity)
- control

Creating an Issue Manually

You can create issues manually at any time you consider this necessary.

To create an issue manually:

1. In the **HOPEX IRM** desktop, select **Test > Remediation > Issues**.
2. Click **New**.
3. Open the properties of the issue.
4. In the **Category** field of the issue, specify if it is an issue detected:
 - at control assessment
 - when performing tests
 - generic

Remediating Issues

To remediate the issue, you must create an action plan.

- For more information on action plans, see [Managing Action Plans for Internal Control](#).

Following Up Issues

You can:

- view issues that have been remediated (of which the action plan is completed)
- generate an issue follow-up report

Viewing remediated / non-remediated issues

To view remediated / non-remediated issues:

1. Click **Test > Remediation > Issues**.
2. In the drop-down list, select:
 - "Closed Issues"
 - "Open Issues"

Generating issue follow-up reports

To generate an issue follow-up report:

1. Click **Analysis > Controls > Remediation**.
2. Click **New** to create a report.
3. In the **Parameters** page, define filter criteria if necessary and select:
 - an entity
 - a process
 - a Begin Date: to obtain issues created after this date
 - an End Date: to obtain issues created before this date
 - *By default the end date is the current date.*
4. Select the **Reports** tab to view the result.
This report shows distribution between issues:
 - remediated
 - non-remediated
 - that do not yet have an action plan

MANAGING ACTION PLANS FOR INTERNAL CONTROL

You can set up action plans to improve a control that has been considered unsatisfactory ("fail").

Creating Action Plans

To create an action plan from an issue:

1. In the **HOPEX IRM** desktop, from the navigation pane select **Test** then open the properties of a test.
2. From the drop-down list, select the **Work Program** page.
3. Select an issue and in its properties, expand the **Action Plans** section.
4. Click **New**.

The action plan is created, as well as its associated workflow.

- For more information on action plan workflows, see [Action Plan Workflows](#).
- The action plan also appears in the following menu: **Test > Remediation > Remediating Action Plans > All Issue-Remediating Action Plans**

You can specify action plan characteristics in its properties. See [Characterizing Action Plans](#).

Characterizing Action Plans

- See also [Creating Action Plans](#).

To specify action plan properties:

1. In the **HOPEX IRM** desktop, select **Test > Remediation > Remediating Action Plans > All Issue-Remediating Action Plans**
2. Open the properties of the action plan.

General characteristics

You can specify the following information:

- **Name:** action plan name.
- **Owner:** by default the user who created the action plan.
- **Owner Entity:** entity responsible for action plan implementation.
- **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"
 - "Critical"
- **Organizational Level:** final objective of plan; this can be:
 - "Global"
 - "Local"
- **Origin:** enables definition of the context of carrying out the action plan:
 - "Audit"
 - "Compliance"
 - "Event"
 - "Risk"
 - "RFC"
 - "Other".
- **Category:** the action plan can for example be connected to:
 - risk impact reduction
 - project management
 - process improvement
 - control performance improvement
 - etc.
- *Other values are available.*
- **Nature:** enables definition of whether the action plan is:
 - Corrective
 - Preventive
- **Comment:** supplements information on the action plan and its characteristics.
- **Steering Calendar:** used for sending reminders to the person responsible for an action plan so that they can indicate action plan progress.
 - *A steering calendar for monthly reminder of progress is supplied by default.*

Financial assertion

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

RACI

The user defined as action plan **Responsible** is responsible for definition of actions to be carried out and their execution.

This field is specified with the name of the action plan creator or with the name of the action plan approver.

- *For more details on the use of RACI, see [Responsibilities concerning Controls](#).*

Success factors

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

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 the following types:

- controls
- applications
- risks
- entities
- processes
- incidents

Milestones

Milestones are key dates of the action plan.

- *The planned end date is mandatory.*

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.*

Managing Actions

The owner of the action plan must define actions enabling execution of the action plan. The owner can create actions and assign these.

-) *An action is included in an action plan and represents a transformation or processing in an organization or system.*

Creating Actions

To create an action from an action plan:

1. In the navigation menu, select **My Tasks > Action Plans/ Recommendations > Action Plans to Implement**.
2. Open the properties of the action plan that interests you.
3. In the **Actions** section, click **New**.
4. In the action properties, complete fields:
 - **Priority**: enables indication of a level. Priority can be: "Low", "Medium", "High" or "Critical".
 - **Owner**: responsible for the action as specified by the action plan creator.
 - **Owner Entity**: entity responsible for action plan implementation.
5. You can specify milestones, which are important dates of the action.
 - **Planned Begin Date**
 - **Planned End Date**
6. Click **OK**.
The action is created with "Created" status.

Defining action scope

An action can concern one or several objects of control, risk or application type.

For example, to define the controls that will be executed in the framework of the action:

1. Open the properties of the action.
2. Expand the **Scope** section.
3. Connect the controls you want to install.

Action Plan Workflows

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

Depending on the profile of the person who 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:*
 - *in the pop-up menu of the action plan from an action plans list*
 - *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](#)

"Top-down" approach

In the framework of a "top-down" approach, the action plan is created by a responsible. The action plan does not need to be validated in this case.

Internal controllers carrying out tests use this approach:

- For the different workflow steps, see ["Top-down" Action Plan Workflow](#)

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](#).

Indicating Action Plan Progress

When the action plan has been started, you can create progress states to indicate its progress.

To specify action plan progress:

1. In the navigation menu, select **My Tasks > Action Plans/ Recommendations > Action Plans to Implement**.
2. Select an action plan and open its properties.
3. Expand the **Action Plan Progress** section, and in the **Progress Update** frame, click **New**.
4. Specify a **Progress Update Percentage**.
5. If required, specify the **Progress Assessment**.
You can specify whether the action plan is:
 - on time, or
 - delayed
6. Click **OK**.
The progress state is created. You can create these at regular intervals.

Action plan follow-up reports

To follow up action plans:

- > Select **Analysis > Action Plans > Follow-Up**.

Access path

Analysis > Action Plans > Action Plan Follow-Up

Result

This report comprises several charts:

- bar charts
- pie charts

The action plans are represented in their different contexts (processes and entities).

Action plans by status

This bar chart presents action plan statuses.

Action plans by progress

This pie chart presents action plan breakdown according to their status. Possible statuses are the following:

- On Time
 - in progress
 - with due date exceeding 30 days
- Delayed:
 - in progress
 - with due date earlier than current date
- Approaching due date:
 - in progress
 - with due date between 0 and 30 days inclusive
- Canceled
- Closed

Action plan by priority

This pie chart presents action plan breakdown according to their priority.

Possible priorities are the following:

- Critical
- High
- Medium
- Low

Action plans by category

This pie chart presents action plan breakdown according to their category.

Possible categories are as follows:

- Corrective
- Preventive

Action plans by entity

This bar chart presents breakdown of action plans for each entity.

- x-axis: all entities
- y-axis: number of action plans linked to each entity and sub-entity
 - *If no entity is selected, all root entities are taken by default.*

Action plans by process

This bar chart presents breakdown of action plans for each process.

- x-axis: all processes (business and organizational)
- y-axis: number of action plans linked to each process and sub-process
 - *If no process is selected, all root processes are taken by default.*

USING HOPEX UCF



HOPEX UCF enables control directors responsible for the implementation of compliance efforts to:

- import data from the UCF Common Controls Hub (Authority Documents, Citations and Common Controls)
- establish what laws and regulations their organization has to comply with
- define the perimeter of entities and processes subject to compliance

- See [UCF Import Prerequisites](#).

- 6 [About Unified Compliance Framework](#)
- 6 [Mapping and Concepts](#)
- 6 [Managing UCF Environment in HOPEX UCF](#)
- 6 [Accessing your Control Framework Library](#)

ABOUT UNIFIED COMPLIANCE FRAMEWORK

UCF (Unified Compliance Framework) is the largest library of regulatory content available today. It contains:

- Authority Documents
- Citations
- UCF Controls

The [Common Controls Hub](#) lets you quickly retrieve the data you need from the underlying [Unified Compliance Framework®](#).

Main Concepts Used in UCF

Authority Documents

An Authority Document is a text that falls under any of following categories:

- regulations (rules of law that, if not followed, can result in penalties),
- guidelines,
- standards,
- best practices.

- *Authority Documents are converted to regulatory frameworks in **HOPEX**. For more details, see [Viewing Regulatory Frameworks](#).*

Citations

Citations are references extracted from the original Authority Documents. They are associated to UCF Controls.

- *Citations are converted to regulation articles or sections in **HOPEX** (depending on whether the Citation is associated to a Mandated Control or not). For more details, see [Viewing Regulation Articles](#).*

- *Citation without any mandate, but containing other Citation becomes a regulation section.*
- *Citation without any mandate and no children Citation become a regulation article that bears no relevance to the organization.*

UCF Controls

Common Controls are the specific steps or actions that must be met to fulfill a compliance mandate stated in a Citation.

- *They are converted to control directives in **HOPEX**. For more details, see [Viewing Control Directives](#).*

Depending on their relations with Citations, different types of UCF controls can be distinguished. For more details, see [Links between UCF concepts](#).

Links between UCF concepts

Enforcement Level is determined by the association of the Common Control to a Citation within a given Authority Document and not by a specific attribute of the Common Control itself.

Citations are associated to UCF Controls, which can be:

- **mandated** (in **bold**)
 - *Only Mandated Controls are mandatory.*
Common Controls become mandated when they are applied to at least one Citation from any Authority Document.
A Common Control that becomes mandated has an impact on the Controls it supports and the Controls that, in turn, support it.
- *implied* (in *italics*)
 - *Implied Controls are UCF Common Controls which are not mandated but contain Mandated Controls in their support structure.*
- Implementation
 - *Controls supporting Controls become 'Implementation Controls'. They provide details not found in Mandated Controls regarding how to carry out the Mandated Control.*

Common Controls		KEY	30 Mandated	22 Implied	931 Implementation
Control Name	ID #				
> Human Resources management	00763				
▼ Privacy protection for information and data	00008				
> Establish and maintain a privacy framework that protects restricted data.	11850				
▼ Establish and maintain a Customer Information Management program.	00084				
> Establish and maintain a customer due diligence program, as necessary.	13618				
Define and assign the data controller's data quality roles and responsibilities.	00085				
> Establish and maintain customer data authentication procedures.	13187				
Check that personal data is complete.	00090				
Keep personal data up-to-date and valid.	00091				
Maintain personal data in a form that does not permit the identification of dat...	00092				

Mandated

Implied

Implementation

Building a Shared List

A Shared List is a selection of Authority Documents that your organization needs to comply with and that you have chosen and saved in the Common Controls Hub workspace.






Lists can be created for documents related to geographic regions of your organization, specific subject matters ("Cybersecurity" or "Banking and Finance"). Select the Authority Documents you need to comply with. All associated Common Controls are automatically displayed in a harmonized, hierarchical list.

- *A Shared List becomes a control framework once imported to HOPEX (a set of regulatory frameworks).*

Make sure your list only includes the Authority Documents you want to import into **HOPEX**.

MAPPING AND CONCEPTS

Mapping between UCF and HOPEX Concepts

UCF	HOPEX	Icon in HOPEX
Authority Document	Regulatory framework	
Citation Without Mandated Control Contains other Citations	Regulation section	
Citation Without Mandated Control	Regulation article	
Citation Without Mandated Control AND without Children	("leaf") Regulation article	
UCF Control	Control directive	

Definitions of Main Concepts Used in HOPEX UCF

HOPEX Concept	Definition
Regulatory framework	A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), guidelines, standards, best practices.

HOPEX Concept	Definition
Regulation article	A regulation article corresponds to a Citation imported from UCF. It is part of a regulatory framework and is usually associated to a control directive.
Regulation section	A regulation section is a citation/text from a regulatory framework without any mandated control directive, but containing other sections or articles.
Control Directive	A control directive, once implemented, enforces any regulation article your organization has to comply with.

MANAGING UCF ENVIRONMENT IN HOPEX UCF

The features available in the **Environment** menu are available to manager profiles only (IRM managers and Control director).

You can:

- Import UCF content from a Shared List built using the Common Controls Hub
- View the resulting regulatory frameworks and control directives in **HOPEX**
- Define what 'mandates' apply to the organization
 - *Once UCF data has been imported into **HOPEX**, it is not possible to export it to transfer it to another repository.*

To manage your UCF environment in **HOPEX**:

- > In the navigation menu, select **Environment > Regulations > Control Framework**.

UCF Import Prerequisites

Internal Control directors or IRM Managers can download UCF content (authority documents, citations and controls) and update it.

To be able to import this content to **HOPEX UCF**, you must have:

- **HOPEX IRM** (or **HOPEX Internal Control** as a minimum) AND **HOPEX UCF**
- a UCF account and API key
- a Shared List with the Authority Documents you want to import.
 - *For more information, see [Unified Compliance Framework](#).*
- parameterized UCF options in **HOPEX UCF**
 - *In the UCF Common Controls Framework, information is generally available in English.*
 - If you want to use **HOPEX UCF** with **HOPEX** user data language other than English, you must:*
 - *set up your data language of interest (example: if you want to use **HOPEX** with French as data language, make sure to set up French as data).*
 - *import UCF data*
 - *repeat the operation (change data language + proceed to import) as many times as desired languages.*

Parameterizing UCF Import

To parameterize UCF import:

1. In the **Main menu**, select **Settings > Options**.

2. In the Options window, expand **Data Exchange > Import > UCF Common Controls Hub Integration**.
3. Select the **Activate UCF Import** check box.
4. Enter the URL corresponding to UCF API.
`https://api.unifiedcompliance.com/`
5. Enter your **UCF API Authentication Key**.
 - To retrieve your API authentication key in your Unified Compliance Framework workspace:
 - go to **Settings > API Manager > API Keys**.
 - **Create Credentials** and copy paste your API Key.
6. Click **OK**.

Importing Data from the Common Controls Hub

Compliance officers need to set up the UCF environment in **HOPEX UCF**. This consists in:

- importing data from the UCF Common Controls Hub (Authority Documents, Citations and Controls)
- declaring the appropriate articles as relevant for your organization: see [Declaring Regulation Content as Relevant](#).

To import UCF data:

1. In the navigation menu, select **Environment > Regulations > Control Framework**.
2. Click **Import UCF content**.
3. Click **Next**.
4. Select the Shared List from your Common Controls Hub.
5. Click **Next**.
6. Select the Authority Document(s) you wish to import into **HOPEX**.

UCF Import - Regulatory Frameworks				
The Authority Documents contained in the previously selected Shared List are displayed below. Please select the Authority Document(s) you wish to import into HOPEX.				
<input type="checkbox"/>	Name ↑	Already Present in HOPEX?	Last Imported UCF Update	Latest Available UCF Update
<input type="checkbox"/>	AICPA Reporting on Controls at a Service Organization SOC-2	No		9/9/2019
<input type="checkbox"/>	Basel II	No		4/2/2020
<input type="checkbox"/>	California Consumer Privacy Act of 2018	No		9/23/2019
<input type="checkbox"/>	EU General Data Protection Regulation (GDPR)	No		9/11/2019

- If you update an already imported Authority Document, it may be useful to compare the columns **Latest available UCF updates** and **Last imported UCF update**.

7. Click **Next**.

For more details on data conversion, see [Mapping and Concepts](#).

Declaring Regulation Content as Relevant

Regulatory content relevance

All the regulatory content of the imported regulatory framework may not be relevant to your organization.

Compliance officers can inspect the imported regulatory framework and specify which parts are relevant.

Only the relevant articles and sections will appear in **HOPEX** libraries for your stakeholders.

Reviewing regulatory frameworks after UCF import

Once the UCF data has been imported, the following tree appears in the **Environment** menu available to manager profiles.

It displays regulatory frameworks (UCF Authority Documents) and features regulation articles (Citations) along their enforcing control directives (UCF Controls). It is based on the supported/supporting structure originally defined by UCF.

From this tree you can:




















- review the newly imported regulatory frameworks and their content.
- Indicate which pieces of regulatory content are deemed relevant to your organization.


Selecting relevant content for your organization

To declare regulatory content as relevant:

1. From the navigation menu, select **Environment > > Regulations > Regulation Framework**.

- Expand the tree if necessary and select the check-box corresponding to the regulatory frameworks/articles/sections you must comply with.

	Relevant	Regulatory Ch
Singapore Personal Data Protection Act 2012 gfuygfuryegfouryeguzryeguregzrte	<input type="checkbox"/>	10
 Part III. GENERAL RULES WITH RESPECT TO PROTECTION OF PERSON...  	<input checked="" type="checkbox"/>	2
  Part III Section 11. Compliance with Act	<input checked="" type="checkbox"/>	5
  Part III Section 11 (2). An organisation is responsible for personal data in its...	<input checked="" type="checkbox"/>	0
  Part III Section 11 (3). An organisation shall designate one or more individu...	<input checked="" type="checkbox"/>	0
  Part III Section 11 (4). An individual designated under subsection (3) may d...	<input checked="" type="checkbox"/>	0
  Part III Section 11 (5). An organisation shall make available to the public the...	<input checked="" type="checkbox"/>	0
  Part III Section 11 (6). The designation of an individual by an organisation u...	<input checked="" type="checkbox"/>	0
  Part III Section 12. Policies and practices	<input checked="" type="checkbox"/>	1
 Part IV. COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA	<input type="checkbox"/>	2
 Part V. ACCESS TO AND CORRECTION OF PERSONAL DATA	<input type="checkbox"/>	2

- The grey square  means that the regulatory content below has been partially selected only.

Data corresponding to the regulatory content you have selected become available to Internal Controllers in the Control Framework libraries. See [Accessing your Control Framework Library](#).

ACCESSING YOUR CONTROL FRAMEWORK LIBRARY

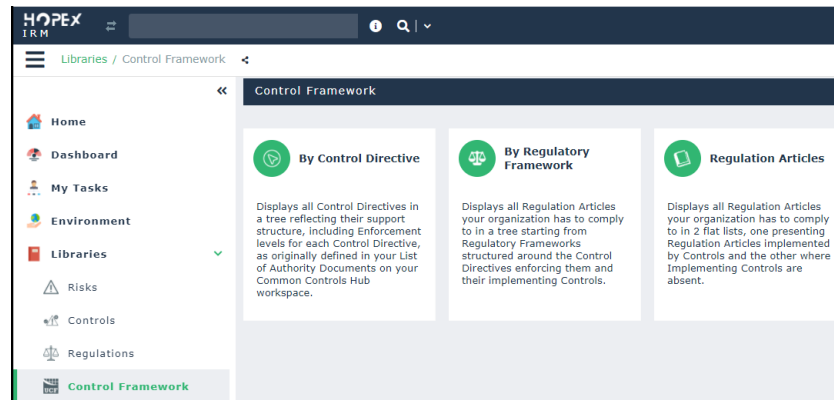
The Control Framework library does not display everything that has been imported from UCF. It only displays the regulatory content the compliance officer has declared as relevant.

Internal controllers can use the Control Framework library to manage the regulatory frameworks, regulation articles and control directives that are applicable to the organization.

- For more details, see [Declaring Regulation Content as Relevant](#).

You can view your control directives through different trees:

- **By control directives**
- **By regulatory frameworks**
- **By regulation articles**



- These object types are created via the UCF Import. They are in read-only mode. Users are not allowed to change legal texts, mandates and best practices. Please note that MEGA is not responsible for the UCF content.

Viewing Regulatory Frameworks

Regulatory frameworks correspond to UCF imported Authority Documents.

A regulatory framework falls under any of following categories:

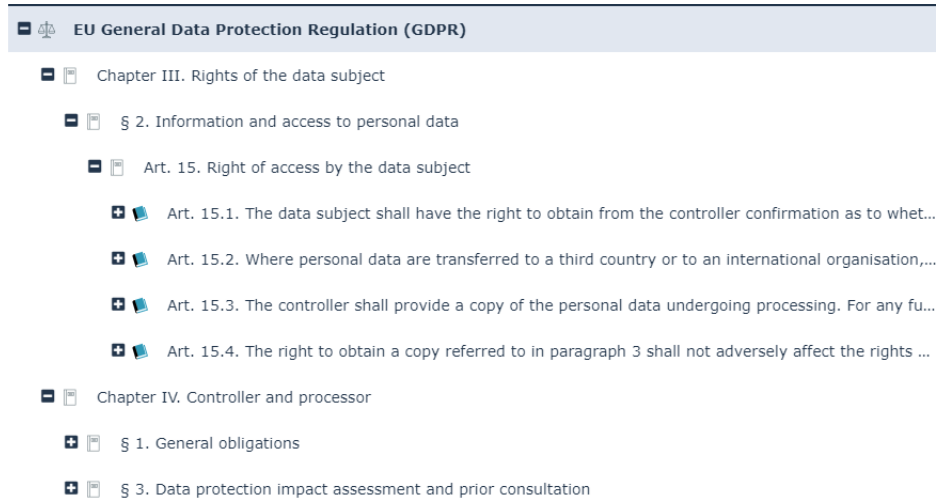
- regulations (rules of law that, if not followed, can result in penalties)
- guidelines
- standards
- best practices

Accessing regulatory frameworks

A regulatory framework tree displays branches of relevant regulation content.

To access the regulation framework tree:

1. In the navigation menu, select **Libraries > Control Framework > By Regulatory Framework**.
2. (optional) Select one regulatory framework from the **Filter by** drop-down list to focus on one regulatory framework only.



- The regulation content displayed corresponds to the content declared as relevant in the **Environment > Regulations > Control Framework**.

The tree starts from the regulatory frameworks and displays:

- the control directives enforcing the regulatory articles
 - For more details on control directives, see [Viewing Control Directives](#).
- The **HOPEX** implementing controls if any

Regulatory framework overview & description

The **Overview** section of the regulatory framework characteristics enables you to display general characteristics originating from the Common Controls Hub.

EU General Data Protection Regulation (GDPR)

Characteristics

Overview

Name
EU General Data Protection Regulation (GDPR)

Published Name
Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulator
European Union

Version

Effective Date
4/27/2016

Release Date
3/8/2018

Regulatory Category
Regulation or Statute

External Identifier(s)
2802

- These characteristics cannot be modified.

Description

URL
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ.L:2016:119:TOC

Description
European Union. Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Issued by EUR-Lex.
This is document has a type of "Regulations" and is mapped as UCF AD ID 0002802 as a part of the Europe category.

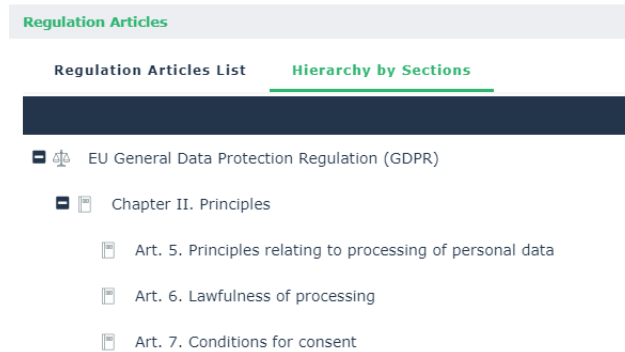
Regulation articles of a regulatory framework

To access the relevant regulation articles of a regulatory framework:

1. In the navigation menu, select **Libraries > Control Framework > By Regulatory Framework**.
2. Select the appropriate regulation framework and open its properties.
3. Expand the **Relevant Regulation Articles** section.

From here you can access relevant regulations articles:

- through a list of **Relevant Regulation Articles**
- through a **Hierarchy of Sections**



Viewing Regulation Articles

Regulation articles correspond to the imported UCF Citations.

- For more details, see [Main Concepts Used in UCF](#).

A regulation article is necessarily associated to a control directive.

- If the original UCF citation has children but is not associated to any UCF Common Control, it becomes a regulation section in **HOPEX UCF**.
If the original UCF citation does not have children and is not associated to any UCF Common Control, it becomes a "leaf" (and irrelevant) regulation article.

The property page of a regulatory article displays:

- the parent regulatory article or section
- children articles, if any
- the elements that are subjected to this regulatory article (entities or processes)
- the associated mandated directives
- the implementing controls, if any

Accessing Regulation Articles

To access regulation articles:

- > In the navigation menu, select **Libraries > Control Framework > By Regulatory Articles**.

The items displayed are classified in two lists:

- **Regulation articles implemented by controls:** relevant regulation articles to be enforced AND implemented by **HOPEX** controls.
- **Regulation articles not implemented by any controls:** relevant regulation articles to be enforced BUT NOT implemented by any **HOPEX** control.

– For more details on **HOPEX** controls, see [Managing Controls](#).

Regulation Articles not implemented by Any Control

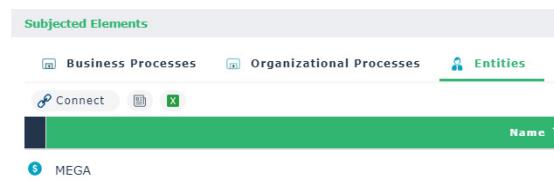
	Name ↑	Regulatory Framework	Control Directives
<input type="checkbox"/>	Art. 15.1. The data subject shall have the right to obtain from the controll...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 15.2. Where personal data are transferred to a third country or to an i...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 15.3. The controller shall provide a copy of the personal data undergoi...	EU General Data Prote...	2
<input type="checkbox"/>	Art. 15.4. The right to obtain a copy referred to in paragraph 3 shall not a...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 25.1. Taking into account the state of the art, the cost of implementati...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 35.1. Where a type of processing in particular using new technologies...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 35.11. Where necessary, the controller shall carry out a review to ass...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 35.2. The controller shall seek the advice of the data protection officer...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 35.8. Compliance with approved codes of conduct referred to in Article...	EU General Data Prote...	1
<input type="checkbox"/>	Art. 35.9. Where appropriate, the controller shall seek the views of data su...	EU General Data Prote...	1

Viewing the objects subjected to a regulation article

Business processes, organizational processes and entities can be associated to regulation articles (or sections) to specify what parts of the organization are subject to compliance.

To connect business processes, organizational processes or entities to a regulation article:

- > In the property page of a regulation article, expand the **Subjected Elements** section and connect objects as appropriate.



– Once connected to the regulation article, the entities, organizational and business processes display a **Regulation Articles** tab in their scope. For more information on entity and process properties, see [Managing Entities](#) and [Managing Processes](#).

Enforcement of a regulatory article

To know more about the enforcement of a regulation article:

- > Open its property pages and expand the **Enforcement** section.

Enforcement		
⌵ Mandated Directives	🔗 Implementing Controls	📄 X
Name ↑	Control Nature	Implementing Controls
⌵ Deliver the records described in the personal data access request, ...	Preventive	0
⌵ Provide personal data in a form that is intelligible.	Preventive	0
⌵ Provide personal data to an individual after the individual's identit...	Preventive	0
⌵ Provide the data subject with a copy of any brochures or other inf...	Preventive	0

You can view:

- its **Mandated Control Directives**
- its **Implementing Controls**
 - *Implied and implementation directives are not connected to any regulation article. You therefore cannot find them in the property page of regulatory articles.*

Mandated directives of a regulatory article

A mandated directive is a directive associated to a regulation article from the regulatory framework(s) selected by the organization. It is considered "mandated" as it enforces a regulatory article.

A regulation article with relevance to the organization is necessarily associated to a mandated control directive.

Implementing controls

Internal controllers must design **HOPEX** controls to implement directives.

- *For more details on implementing controls in **HOPEX**, see [Managing Controls](#).*

Connecting Business Documents

You can link business documents to an article (or a section).

Viewing Control Directives

Control directives correspond to the imported UCF Controls.

- *For more details, see [Main Concepts Used in UCF](#).*

Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

Accessing control directives

To access control directives from a tree:

- > In the navigation menu, select **Libraries > Control Framework > By Control Directive**.

Enforcement		
<div> Mandated Directives Implementing Controls </div>		
Name ↑	Control Nature	Implementing Controls
Deliver the records described in the personal data access request, ...	Preventive	0
Provide personal data in a form that is intelligible.	Preventive	0
Provide personal data to an individual after the individual's identit...	Preventive	0
Provide the data subject with a copy of any brochures or other inf...	Preventive	0

- *First-level Implied control directives appear in this list only if one of their children is mandated.*

The following information is displayed for each control directive:

- **Enforcement Level**
 - See [Enforcement level of control directives](#).
- Number of **Supporting Directives**.
 - See [Supported and supporting directives](#).

Information is also given on **HOPEX** controls implementing each control directive:

- Number of **Implementing Controls**.
- **Execution rate**
 - *The execution rate relates to control execution check-lists. It indicates the percentage of controllers which have successfully executed the controls implementing the control directive.*
- **Control pass level**: gives an indication on how adequate and how effective the control is (Control Design (IC) * Control Efficiency (IC)).
 - *For more details on control contextualization see [Executing controls](#).*

Viewing fulfilled regulation articles

A mandated control directive is associated to a regulation article.

It is beneficial to have several regulation articles in the **Fulfilled Regulation Articles** section of a control directive. It means that your control directives enforce compliance of your organization to several regulation articles.

Establish and maintain a personal data transparency and openness program.

Characteristics

Name

Control Framework::Establish and maintain a personal data transparency and openness program.

Overview

Name

Establish and maintain a personal data transparency and openness program.

Control Nature

Preventive

Enforcement Level

▼

Mandated Control

External Identifier(s)

375

Fulfilled Regulation Articles

X

Name ↑

Art. 40.2.(a). fair and transparent processing;

Art. 5.1.(a). processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness

Supported and supporting directives

All control directives are presented in a tree structured around the control directives supporting one another, as originally defined in the UCF Common Control Framework.

130

The screenshot displays the HOPEX UCF interface. On the left, a list of control directives is shown. The selected directive, "Establish and maintain a Customer Information Management program," is highlighted. Below it, a list of supporting directives is displayed. On the right, the detailed view of the selected directive is shown, including its name, characteristics, control nature, enforcement level, and external identifier(s). The "Supported & Supporting Directives" section is also visible, showing the selected directive and its supporting directives.

Annotations:

- Supported directive
- Directive
- Supporting directives

Having several control directives in the **Supported Directive** tab of a control directive is highly beneficial. This means that efforts spent implementing one mandated control directive also contributes partly to the implementation of its supported control directives.

Enforcement level of control directives

There are three enforcement levels for each control directive:

- **mandated**
 -) a mandated directive is directly associated to a regulation article. It implements a regulatory framework.
- **implied**
 -) An implied directive is a non-mandated control directive that is a parent of a mandated directive. It indicates that one of the control directives contained within its supporting hierarchy is mandated.
- **implementation**
 -) An implementation directive is a non-mandated directive that is a child of a mandated directive. It provides details regarding how to carry out the mandated directive and facilitates its implementation.

Enforcement level for control directives	
Implied control directive	<ul style="list-style-type: none">- Is not mandated- Contains at least a mandated control directive in its hierarchy- Allows to display the mandated control directives within the UCF hierarchy- Is supported by a mandated control directive
Implementation control directive	<ul style="list-style-type: none">- Is not mandated- Appears under a mandated control directive (is supporting a mandated control directive)
Mandated control directive	<ul style="list-style-type: none">- Is supporting an implied control directive- Can be supported by implementation control directives- Can support or be supported by other mandated directives

Viewing HOPEX controls implementing a control directive

Columns in the list of control directives give you an overview of **HOPEX** controls that are actually implementing each control directive.

To have a more detailed view of the controls implementing a control directive:

1. In the navigation menu, select **Libraries > Control Framework > By Control Directive**.
2. Open the properties of a control directive.
3. Expand the **Implementation** section.

You are given information on the control as well as on its execution results:

- **Control nature**
- **Aggregated Execution Rate**
 - The execution rate relates to control execution check-lists. It indicates the percentage of controllers who have successfully executed this control whatever the context.
- **Control Pass Level**
 - For more details on control contextualization see [Executing controls](#).

Connecting Business Documents

You can attach business documents in the properties of a control directive.



HOPEX Enterprise Risk Management



CONTENTS



Contents	1
---------------------------	----------

Managing Risks	5
---------------------------------	----------

Risk Management Profiles	6
---	----------

Creating a Risk	7
----------------------------------	----------

Assessing risks	8
----------------------------------	----------

All Risks	8
---------------------	---

Risks by Taxonomy	8
-----------------------------	---

Risks by Context	8
----------------------------	---

Risks by Mitigation	9
-------------------------------	---

Risks by Materialization	9
------------------------------------	---

<i>Risks with Open Incidents</i>	9
--	---

<i>Materialized Risks</i>	9
-------------------------------------	---

<i>Unmaterialized Risks</i>	9
---------------------------------------	---

Risk characteristics	10
---------------------------------------	-----------

General characteristics	10
-----------------------------------	----

Risk, factors and consequences	10
--	----

<i>Risk types</i>	11
-----------------------------	----

<i>Risk factors</i>	11
-------------------------------	----

<i>Risk consequences</i>	12
------------------------------------	----

RACI on a Risk	12
--------------------------	----

Risk Dashboard	12
--------------------------	----

Contextualizing Risks	13
Risk Workflow	14

Assessing Risks **15**

Risk Assessment Types	16
Assessing risks directly	17
Direct Assessment Context	17
Direct Risk Assessment Templates	17
<i>Assessed characteristics</i>	17
<i>Assessed objects</i>	18
<i>Respondents</i>	18
<i>Questionnaire</i>	18
Creating a Direct Assessment on a Risk	18
Assessing Multiple Risks Simultaneously	20
Viewing and Analyzing Risk Assessment Results	24
Displaying Risk Assessment Results	24
Generating Reports on Assessments	24
<i>Instant reports</i>	24
<i>Generating dedicated reports</i>	25

Treating Risks **27**

Risk Treatment Mode	28
<i>Risk Treatment Decision</i>	28
<i>Risk levels</i>	29
Actions to Treat Risks	30
<i>Specifying treatment actions</i>	30
<i>Setting up action plans</i>	31
<i>Control policy monitoring</i>	31

Report Related to Risks **33**

Risk Environment Report	34
<i>Access path</i>	34
<i>Report parameters</i>	34
<i>Creating a Risk Environment Report</i>	35
Incident Identification Reports	37
Location Matrix	37
<i>Access path</i>	37
<i>Report parameters</i>	37
<i>Report example</i>	38
Risk identification	38

Access path.	38
Report parameters.	38
Report example.	39
Aggregation Reports.	42
Net Risk by Risk Type	42
Access path.	42
Risk Heatmap (Aggregated)	42
Access path.	42
Report parameters.	42
Content of the heatmap	42
HeatMap by Entity/Risk Type/Process.	43
Access path.	43
Report parameters.	44
Report example.	44
Assessments per Context	45
Access path.	45
Report parameters.	45
Overall Risk Level by Process	45
Access path.	45
Report parameters.	46
Report example.	46
Overall Risk Level by Entity	46
Access path.	46
Report parameters.	47
Report example.	47
Aggregation Report	47
Access path.	48
Report parameters.	48
Report example.	48
Risk Follow-Up Reports	50
Session Statistics	50
Access path.	50
Parameters	50
Report example.	51
Result	51
Risk Management Effectiveness Reports	52
Risk Context Synthesis	52
Access path.	52
Parameters	52
Report content	52
Risk Reduction	53
Access path.	53
Report parameters.	53
Report example.	53
Coverage & Risks Matrix	54
Access path.	54
Matrix content.	54
Trend Analysis	55
Access path.	55
Report parameters.	55
Report example.	55

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:

- 6 [Risk Management Profiles](#)
- 6 [Creating a Risk](#)
- 6 [Accessing risks](#)
- 6 [Risk characteristics](#)
- 6 [Risk Workflow](#)

RISK MANAGEMENT PROFILES

To connect to HOPEX, see **HOPEX Common Features**, "HOPEX desktop", "Accessing HOPEX (Web Front-End)".

Profiles	Desktop	Tasks
Risk Manager (Or GRC manager)	HOPEX IRM	The Risk Manager is responsible for executing the following tasks on risks within his responsibility domain: <ul style="list-style-type: none"> - identifying risks - carrying out direct assessments - managing assessment campaigns - defining action plans - analyzing and following report creation
GRC Contributor (Lite)	IRM Contributors	Use the simplified HOPEX Explorer desktop. <ul style="list-style-type: none"> - answer assessment questionnaires - define action plans See The IRM Contributor Desktop .

- For more details, see also [Accessing the IRM Manager Desktop](#).

CREATING A RISK

To create a risk:

1. In the navigation menu of the **HOPEX IRM** desktop, select **Libraries > Risk Library > All Risks**.
You obtain the list of all risks.
2. Click the **New** button.
3. Open its properties page.
4. Specify the risk **Owner** responsible for entering information on the risk before submitting it for validation.

See also:

- [Risk characteristics](#)
- [Risk Workflow](#)

ACCESSING RISKS

To access risks according to different criteria:

- > In the **HOPEX IRM** desktop, select **Libraries > Risk Library > All Risks**.

All Risks

Risks can be classified according to different criteria:

- All Risks in My Environment
- Risks to Review
 - *This list displays the risks which were submitted and which need to be reviewed by the manager.*
- Risks without Recent Assessment
 - *This list displays risks which have never been assessed or which have not been assessed for the last 12 months.*
- Risks with High Net Risk
 - *The net risk indicates the risk to which the organization remains exposed after management has processed the risk.*
- Key Risks in My Environment
 - *Key risks are the risks for which the **Key Risk** check box was selected in the risk properties page.*

Risks by Taxonomy

This list displays all Risks in your environment in a tree structured around Risk Types.

For each risk type, columns display:

- The number of sub-risk types
- The number of risks

Risks by Context

The risks of your environment are classified as a function of the context:

- Without context
- By process
- by entity
- By business line
- by application

Risks by Mitigation

Risks are grouped by mitigation method (controls or action plans):

- Risks with or without Action Plans
- Risk with Delayed Action Plans
 - *The planned end date is the most distant planned end date of all delayed Action Plans for the displayed Risk.*
- Risks mitigated by Controls
- Risks Without Control.
 - *This list displays risks which are not mitigated by controls.*

Risks by Materialization

Risks are grouped by incident materializing risks or by open incident.

Risks with Open Incidents

Displays risks with at least one incident connected (which is not in Closed, Rejected, or Draft status).

Materialized Risks

A materialized risk is a risk which is connected to at least one incident.

- *The net risk displayed here is the sum of net losses of all incidents declared for the risk.*

Unmaterialized Risks

This list displays risks which are not connected to any incident.

RISK CHARACTERISTICS

- 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 Assessment Work Environment](#).

General characteristics

To access characteristics of a risk:

- > Select a risk from a list of risks or key risks and click the **Properties** button.

The properties page of the risk appears in the right pane.

On this page you can specify for the control:

- the risk identification **Code**
- the risk **Name**
- the fact that the risk is high level by selecting the **Key Risk** check box
- the risk **Owner**
- the risk **Identification Mode**

The risk could have been identified from:

- an "incident database"
- a "workshop"
- a "survey"
- an "audit"
- the risk **Description**

- The risk **Status** cannot be modified since it is managed by the workflow associated with the risk.

See also:

- [Risk, factors and consequences](#)
- [RACI on a Risk](#)
- [Risk Dashboard](#)
- [Contextualizing Risks](#) (scoping risks)

Risk, factors and consequences

The aim of risk analysis is to obtain a good understanding of risks. You need to take into account:

- risk causes
- positive or negative risk consequences

The risk analysis phase associates a risk with:

- risk types
- risk factors
- consequences
- other risks

To analyze a risk:

1. Select a risk and open its properties.
2. In the **Characteristics** tab, expand the **Analysis** section.

A risk is characterized by:

- **Risk Types:** for more details, see [Risk types](#).
) A risk type defines a risk typology standardized within the context of an organization.
- **Risk Factors:** for more details, see [Risk factors](#).
) A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...
- **Risk Consequences:** for more details, see [Risk consequences](#).
) A risk consequence can be positive or negative. It is associated with a type, which enables its characterization, for example: image, environment, employees.
- **Related Risks**
- **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.

Risk types

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

A risk type enables risk characterization. For example, a risk type can be regulatory, legal, technical, etc.

To create your own risk types:

1. In the navigation menu, click **My Environment > Risk Environment > All Risk Types**.
2. In the pop-up menu of the "Risk Type" folder, select **New**.
3. Enter the name of the risk type and click **OK**.
 The new risk type appears in the navigator menu tree.
 - Similarly, you can create a sub-risk type from a risk type.

Risk factors

Many risk factors are defined within the framework of international, national or inter-professional regulations, or within the enterprise itself.

) A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the

complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...

With each risk, you can associate one or more risk factors, sources of risks that have intrinsic potential to endanger organization operation. For example, dangerous chemical products, competitors, governments, etc.

Risk consequences

To define consequences associated with a risk:

- > In the risk page, **Analysis** section, **Risk Consequences** tab, click **New**. The consequence creation page appears.
 - *Since a risk consequence can relate only to a single risk, the **Risk** field is already entered with the current risk.*

The consequence created appears in the list of consequences associated with the risk.

RACI on a Risk

A risk properties page includes an **RACI** section to define the different persons responsible for risk management. For more details, see [RACI Responsibilities](#).

See also:

- [Contextualizing Risks](#)
- [Risk, factors and consequences](#)
- [Risk Dashboard](#)

Risk Dashboard

A number of indicators are available in the **Characteristics** page of risk properties.

- **Assessment Freshness**: elapsed time (number of months) since the last assessment (either direct assessment or through campaigns)
 - *This is an indicator of how often a risk is assessed. This can be useful when it comes to decide when to perform the next assessment.*
- **Aggregated Net Risk**: average of the net risk from the latest risk assessment session. All contexts for which the risk was assessed during the last assessment session are considered (e.g. org-unit, processes, application...) and the average is computed.
 -) *The net risk indicates the risk to which the organization remains exposed after management has processed the risk.*
- **Open incidents**: number of incidents corresponding to risks having a status other than "closed".
 - *See the [Collecting Incidents](#) guide for more details on incidents.*
- **Next year Forecast**: represents the net risk forecast for the year to come (average net risk)

CONTEXTUALIZING RISKS

Contextualizing a risk consists in defining its scope. Different types of components can be included in the scope.

To contextualize a risk:

- > In the properties of a risk, expand the **Scope** section and connect objects in the relevant tabs.
- **Entities** concerned by the risk. For more details, see [Managing Entities](#).
 -) *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.*
 - *Defining entities on risks is a pre-requisite to risk assessment. See also [Preparing the Assessment Work Environment](#).*
- **Business Processes** and **Organizational Processes** exposed to the risk. For more details, see [Managing Processes](#).
 -) *A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.*
 -) *An organizational process describes how to implement all or part of the process required to make a product or handle a flow.*
- **Objectives and Requirements** expected related to risk management. For more details, see [Consulting Requirements](#).
 -) *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.*
 -) *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.*
- **Applications**: for more details, see [Managing Applications](#).
 -) *An application is a set of software tools coherent from a software development viewpoint.*
- **Business Lines**: for more details, see [Managing Business Lines](#).
 -) *A business line is a skill or grouping of skills of interest for the enterprise. It corresponds for example to major product segments, to distribution channels or to business activities.*

RISK WORKFLOW

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, see [Risk Workflows](#).

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.

ASSESSING RISKS



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 IRM**, 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.

- *This chapter explains how to start assessments. To configure these, see the **HOPEX Power Studio** guide > Customizing Assessments > Assessment Templates".*

- 6 [Risk Assessment Types](#)
- 6 [Assessing risks directly](#)
- 6 [Viewing and Analyzing Risk Assessment Results](#)

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: for more details see [Creating a Direct Assessment on a Risk](#)
- From a multiple assessment table: see [Assessing Multiple Risks Simultaneously](#).
- Through an assessment questionnaire sent to appropriate recipients: see [Risk and Control Campaign Assessment](#).

Results of risk assessment can be displayed in dedicated reports which make it easier to analyse the assessed risks. For more details, see [Report Related to Risks](#).

ASSESSING RISKS DIRECTLY

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

Direct Assessment Context

In direct assessment, the values of the characteristics can be specified in two ways:

- in the properties of each risk
- globally, using a multiple assessment table

Direct assessment is carried out for all context objects available in the **Scope** section of the risk properties window:

- Organizational processes
- Business processes
- Entities
- etc.

Direct Risk Assessment Templates

The **HOPEX IRM** solutions provide risk assessment templates in the context of the following objects:

- an org-unit
- a business process
- an organizational process
- an application
- a business line

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: Criticality.*

Example of assessed characteristics:

- Impact
- Likelihood
- Control Level
 -) *Control level characterizes efficiency level of control elements deployed (controls) to assess the risk.*
- Net risk
 -) *The net risk indicates the risk to which the organization remains exposed after management has processed the risk.*

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

) *An assessment questionnaire is a list of questions relating to a particular object and addressed to users.*

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.*

Creating a Direct Assessment on a Risk

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

This is an "expert view" assessment.

To create a direct assessment on a risk:

1. Select the risk and open its properties.
2. Select the **Assessment** tab.
3. Click the **Perform Assessment** button.
 - *The **Perform Assessment** button is available if the risk has been contextualized accordingly.*
4. If several contexts are available for the risk, select the context(s) for which you want to assess the risk and click **Next**.
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 **Measure Date** if necessary.
7. Click **OK**.

An assessment is created.

Through the multiple assessment table you can specify the same value for several assessment nodes of different risks.

To assess several risks simultaneously:

1. From the navigation menu click **Assessment > Direct Assessment > Risk Multiple Assessment Table**.
2. In the window that appears, click the **Launch Multiple Assessment** button.
3. In the **Context Element** field, select the object type which makes up the risk assessment context.
 - org-unit
 - application
 - business line
 - business processes
 - organizational processes

The **Assessment Template** corresponding to the selected type context is indicated.

Multiple Assessment - Select Context Element & Template

+x

i

To build a new Multiple Assessment Table, first select the relevant context element.

Context Element

Business Process

▼

i

Select the relevant assessment template. Available options are determined by the previously selected context element.

Assessment Template *

Risk Assessment per Business Process

▼

i

Assesses Risks in the context of Business Processes using the following criteria:

- Impact
- Likelihood
- Control Level

4. Click **Next**.

- In the displayed tree, select the objects that define the assessment context.
A risk is assessed in the context of elements of the branch from the risk up to the root.

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

6. Click **OK**.
- If assessments have already been carried out, the most recent assessment values are presented in columns.

7. For each assessed object select the appropriate assessed characteristic values:
 - **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.
 - *All assessed objects for which you have given answers become green.*
8. When you have answered all the questions, click **OK**.

Validation automatically creates an assessment in the **Assessment** page of the control properties. For more details, see [Displaying Risk Assessment Results](#).

VIEWING AND ANALYZING RISK ASSESSMENT RESULTS

Displaying Risk Assessment Results

To display the results of assessments performed on a risk:

1. From the risk library, select the **Assessment** page of the risk properties.
2. (optional) In the **Assessment Results** section, select the context element and template you are interested in and click **Apply filters**. The corresponding assessments appear. This way you can filter assessments when there are a lot of them.

For each assessment node the following values are calculated:

- inherent risk
) *The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact of this risk.*
- net risk
) *The net risk indicates the risk to which the organization remains exposed after management has processed the risk.*

Generating Reports on Assessments

Instant reports

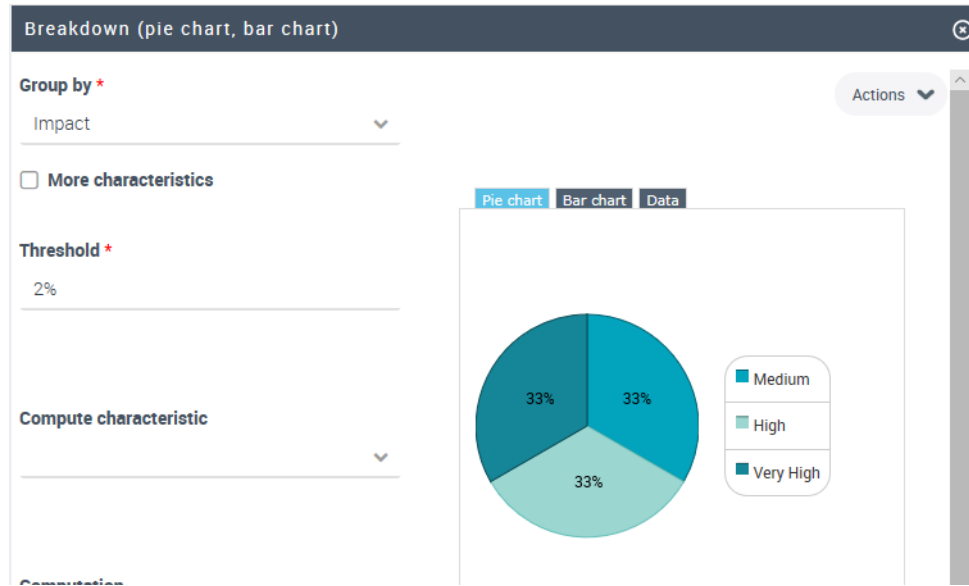
Instant reports offer a statistical graphic analysis of the data. You can generate instant reports on a selection of assessments in order to view certain data graphically or to compare the assessments for specific characteristics.

To launch an instant report on a set of assessment of a risk:

1. Display the properties of the risk and click the **Assessment** page.
2. Select the assessments in question.
3. Click the **Instant Report** button.
4. Select the type of report to create and then, if necessary, the characteristics to be analyzed.

Example

Find below an example of breakdown report on risks. From the selected characteristics (risk impact in this example), this report offers a graphical representation of results.



For more details on instant reports, see the HOPEX Common Features user guide, "Generating Documentation", "Managing Instant Reports".

Generating dedicated reports

In addition to instant reports, **HOPEX IRM** provides dedicated report templates that facilitate the analysis of the assessed risks. For more details, see ["Report Related to Risks"](#), page 33.



TREATING 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 treating risks.

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

RISK TREATMENT MODE

To specify risk treatment choices:

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

Bad Image Impact

⚠ | Treatment ▾

Treatment Decision

Target Risk

■ Low ▾

☐ Acceptance

☐ Reduction

☐ Transfer

☐ Insurance

Risk Treatment Decision

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 treat 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.
- **Assurance**
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 treatment should be the solution that brings risk within the tolerable limit required by management.

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

ACTIONS TO TREAT RISKS

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.

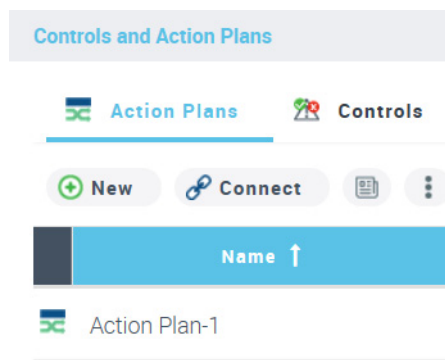
In the case of transfer to partners or assurance, we can specify contracts to be agreed with them, as well as the predicted impact on organization processes.

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

Specifying treatment actions

To indicate the controls and action plans enabling risk prevention:

- > In the **Treatment** page of the risk properties, 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 being to reduce risks and events that have a negative impact on company activities.*
 - 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.

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.

For more information on action plan workflows, see [Action Plan Workflows](#).

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.

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 processes
 - applications
- Object types enabling the indication of control implementation responsibilities.

For more details on controls, see ["Managing Controls", page 13](#).

REPORT RELATED TO RISKS



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

- 6 [Risk Environment Report](#)
- 6 [Incident Identification Reports](#)
- 6 [Aggregation Reports](#)
- 6 [Risk Follow-Up Reports](#)
- 6 [Risk Management Effectiveness Reports](#)

RISK ENVIRONMENT REPORT

- This report is available for all ERM profiles.

You can choose to display the following elements for a given risk:

- the risk context
 - business processes
 - organizational processes
 - applications
 - Org-Units
 - business lines
- the strategic objects impacted by the risk:
 - objectives
 - requirements
- the consequences of the risk
 - target risks
- the preventive controls designed to mitigate the risk
 -) A control is a set of rules and means enabling the assurance that a legal, regulatory, internal or strategic requirement is respected.
- 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.

Access path

Risk properties (**Reporting > Risk Environment**)

Report parameters

Parameters	Parameter type	Constraints
Risk	1 risk	Mandatory
Risk Context	Check Box	Optional
Objectives and Requirements	Check Box	Optional
Target Risks	Check Box	Optional
Controls	Check Box	Optional
Incidents	Check Box	Optional

Parameters	Parameter type	Constraints
Findings	Check Box	Optional
Action Plans	Check Box	Optional
Actions	Check Box	Optional

Creating a Risk Environment Report

To display a risk environment report:

1. In risk properties, select the **Reporting > Risk Environment** page.
2. In the **Parameters** section, select the types of environment objects that you wish to display.

Bad Image Impact

⚠️ | Reporting ▼

Risk Environment ▼

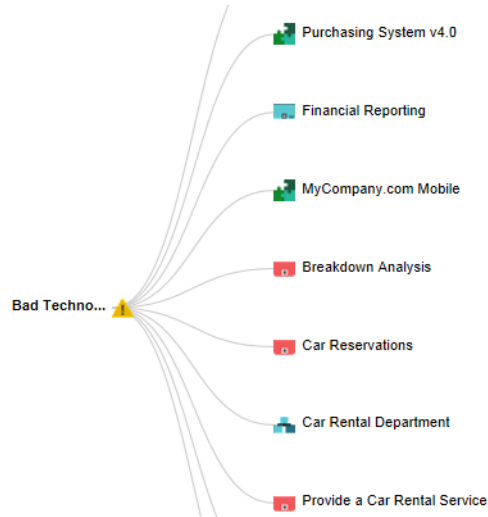
Parameters

☒ Risk context (Business Processes, Organizational Processes, Applications, Org-units, Business Lines)
 ☐ Objectives and Requirements
 ☐ Target Risks
 ☐ Controls
 ☐ Incidents
 ☐ Findings
 ☐ Action Plans
 ☐ Actions

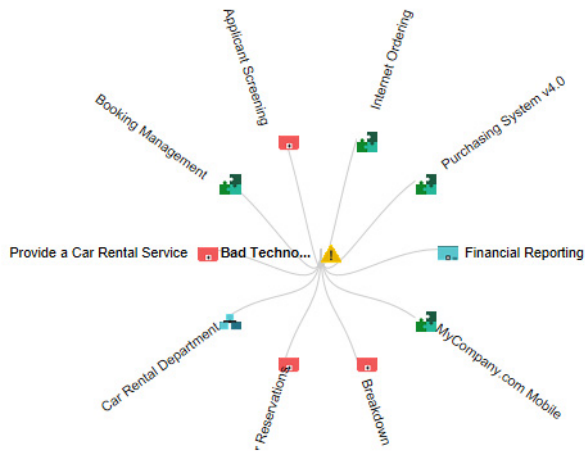
Display *

Horizontal ▼

3. In the **Display** field, specify whether you want to display the risk environment objects:
- in a horizontal fashion, or,



- in a circular fashion (based on the selected risk)



4. Click **Refresh**.

Using this diagram, you can:

- fold/unfold the branches
- open the properties page of the selected object.

INCIDENT 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

Access path

Analysis > Risks > 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*.

Sub-entities of the root entity



	Belgium	Canada	France	Germany	Italy
▲ *Risk of non-payment			✓	✓	✓
▲ Application Hack			✓		
▲ CO2 emissions			✓		
▲ Credit card risk		✓			✓
▲ Damage to physical assets		✓			✓
▲ Data encryption	✓				
▲ Data Transmission					
▲ Double payment					
▲ Economic crisis					✓
▲ Fraud & Corruption	✓		✓		
▲ Fraud: unregistered call for tender					
▲ Fraud: wrong registering					
▲ Insufficient budget	✓				
▲ Liquidity risk					
▲ Natural catastrophe			✓		

Risk identification

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

Access path

Analysis > Risks > Identification > Risk Identification

Report parameters

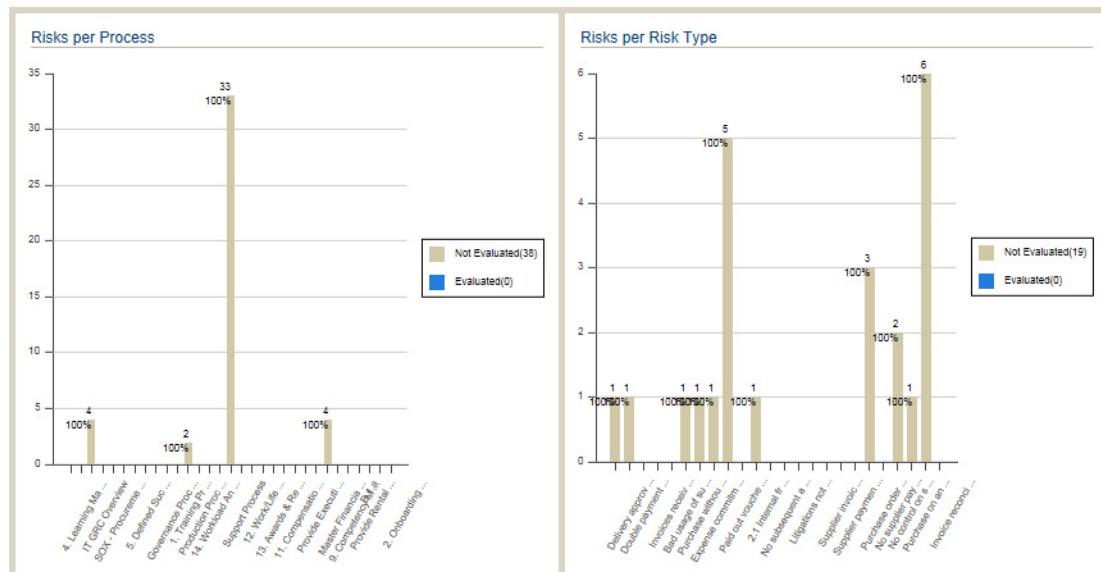
This consists of selecting risks that will be presented by specifying elements that define their scope: risk types, entities, processes or objectives.

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.

Report example

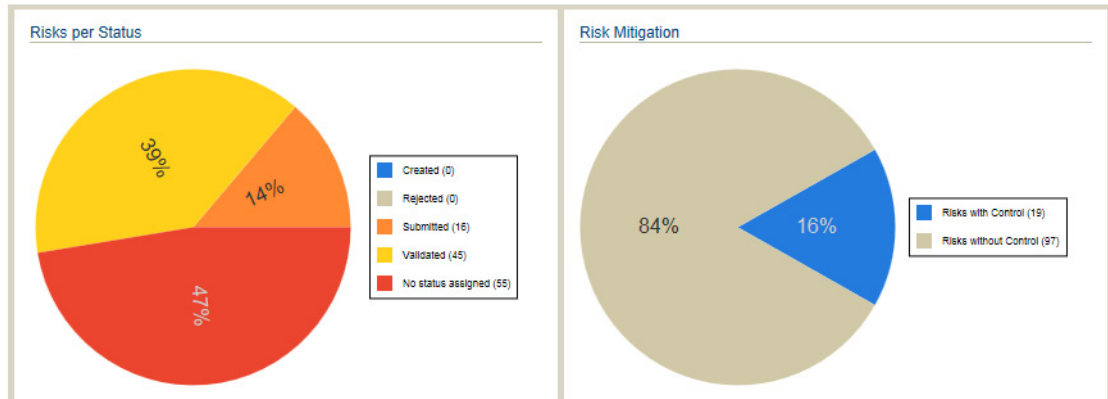
The upper part of the report presents distribution of risks on the following criteria:

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



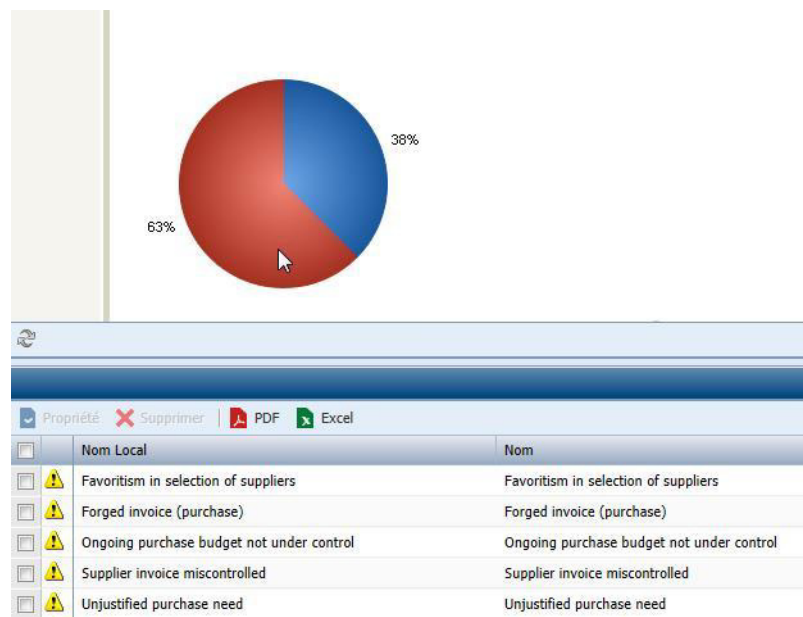
The lower part of the report presents distribution of risks on the following criteria:

- 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.

AGGREGATION REPORTS

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 net risk indicates the risk to which the organization remains exposed after management has processed the risk.*

Access path

Analysis > Risks > Aggregation > Net Risk by Risk Type

Risk Heatmap (Aggregated)

The Risk Manager as well as all contributors can display the impact and the likelihood of a set of risks.

- *Aggregation consists of calculating an aggregated value of the values specified on each risk based on assessments.*

Access path

Analysis > Risks > Aggregation > Risk Heatmap (aggregated)

Report parameters

To specify the report parameters:

- > After creating the report, in the **Parameters** tab, specify the **List of Risks** that will populate the report.

Content of the heatmap

To display the report content:

- > After specifying the report parameters, select the **Reports** tab.

This heatmap displays the aggregated values of risks without risk duplication (as context is not taken into account).

Impact/Likelihood

	Rare	Possible	Likely	Probable	Certain	Sum
Very High	1	0	4	3	6	14
High	2	3	1	5	2	13
Medium	4	5	4	2	4	19
Low	3	6	5	4	0	18
Very Low	2	2	2	3	1	10
Sum	12	16	16	17	13	

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.

Access path

Analysis > Risks > 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.
List of risk types	Risk type	Risk selection criterion. Not mandatory.
List of org-units	entity	Risk selection criterion. Not mandatory.
List of processes	process	Risk selection criterion. Not mandatory.
List of objectives	objectives	Risk selection criterion. Not mandatory.
List of control systems	Control systems	Risk selection criterion. Not mandatory.

- If you complete a risk type and an entity, 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						Control Level /Inherent Risk				
	Rare	Possible	Likely	Probable	Certain		Very Low	Low	Medium	High
Very High	0	0	0	0	0	0	Very Weak	0	0	0
High	0	0	0	0	0	0	Weak	0	0	0
Medium	0	0	0	0	0	0	Medium	0	3	0
Low	0	1	0	0	0	1	Strong	0	1	0
Very Low	0	2	0	1	0	3	Very Strong	0	0	0
Total	0	3	0	1	0	4	Total	0	4	0

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

Assessments per Context

This report enables to display risk assessment results by:

- business processes
- objective
- org-unit
- Risk type

Access path

Analysis > Risks > Aggregation > Assessments per Context

Report parameters

Parameters	Parameter type
Begin Date	Date
End date	Date
Context type	Business processes Objective Org Unit Risk Type

Overall Risk Level by Process

This report displays a table of risks linked to the objectives of business processes specified as a parameter.

It displays values of net risk for each risk in each business process.

Access path

Analysis > Risks > Aggregation > Overall Risk Level Per Process

Report parameters

Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
List of business processes	Business processes	Risk selection criterion. Not mandatory.

Report example

Action Plan	Current Average Net Risk Level	Max Risk Level	Min Risk Level	Objectives	Risk	Target Average Risk	
Process	Objectives	Risk	Target Average Risk	Current Average Net Risk Level	Min Risk Level	Max Risk Level	Action Plan
 Car Repair Process	 Improve Quality of Service	 *Risk of non-payment	 Low				 *Improve control on Projects Loan Management
 Provide Vacation Service	 Deliver Booking Services on EMEA Destinations	 Invoice approved without valid justification	 Very Low				 Verification of purchase orders and invoices
		 Invoice without corresponding goods or services	 Very Low				
		 IT Access to Purchase Order is impossible					
		 Ongoing purchase budget not under control	 High				
		 Overdue contractual delivery date	 Low				 Annual Review of supplier contracts

Overall Risk Level by Entity

This report displays a table of risks linked to the objectives of entities specified as a parameter.

It displays values of net risk for each risk in each entity.

Access path

Analysis > Risks > Aggregation > Overall Risk Level Per Entity

Report parameters

Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Number of Entities	Entities	Risk selection criterion. Not mandatory.

Report example

<div> Action Plan ▼ Current Average Net Risk Level-1 ▼ Max Risk Level ▼ Min Risk Level ▼ Objectifs ▼ Risk ▼ Target Average Risk ▼ </div>							
Org-Unit	Objectifs	Risk	Target Average Risk	Current Average Net Risk Level	Min Risk Level	Max Risk Level	Action Plan
France	30% revenue by internet in 2016	*Risk of non-payment					Improve control on Projects Loan Management
		Fraud & Corruption					Get a budget extension
		Production delays					
Italy	100% of top 10 packages delivered by internal staff by 2013	Application Hack	2 Low				
		Bad Technology Choices					
		Creation of an imaginary supplier	3 Medium				
		Damage to physical assets					
		Duplicate invoice paid	1 Low				Verification of purchase orders and invoices
		Favoritism in selection of suppliers	2 Low				
		Production delays					

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

Analysis > Risks > 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 anonymous 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

RISK FOLLOW-UP REPORTS

Session Statistics

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

Access path

Analysis > Risks > Follow-Up

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%
Damage 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 REPORTS

Risk Context Synthesis

The Risk Manager uses this report to display:

- the risks impacting the entity for which he/she is responsible as well as its sub-entities
- The environment objects for each risk (business process and/or business line, for example)
- the mitigation status of risks managed
 - the mitigation controls
 - the incidents that determine these risks
 - the action plans concerning the risks

If, for example, the risk is gives birth to incidents, the Risk Manager can display which action plans to modify.

Access path

Analysis > Risks > Effectiveness > Risk Context Synthesis

Parameters

Parameters	Constraints
Elements at risk	Mandatory

Report content

The reports display the following in columns:

- the elements at risk (for example sites or organizational processes)
- The associated risks
- The date of the last risk assessment
- Any incidents
- The date the incident took place
- Related controls
- The action plans to implement
- End date of action plan

Risk Reduction

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

Access path


















Analysis > Risks > Effectiveness > Risk Reduction

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.
Processes	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 catastrophe	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

Coverage & Risks Matrix

As a Risk Manager, you must ensure the risks in your scope have associated mitigating controls. This will allow you to prioritize your control design efforts.

Access path

Analysis > Risks > Effectiveness > Risk and Control Coverage Matrix

Matrix content

This matrix displays:

- all the risks in the scope of the Risk Manager
- the controls whose purpose is to mitigate these risks
 - The intersection between the rows and columns indicates that the control mitigates the risk.

	Approval of needs control Debt level	Followup of refused receptions Only Purchasing Mgr (and Backup) Update Supplier Characteristics Payments control	Providers approval
▲ Architecture lacks flexibility			
▲ Car breakdown			
▲ Default of payment	✓		✓
▲ Financial Health	Unknown / Very Strong		
▲ Fraud: unregistered call for tender			Unknown / Very Strong
▲ Insufficient budget			
▲ Insufficient market analysis			

Risk mitigated by a control

Risk not mitigated by any control

Inherent Risk / Control Level

When a risk is mitigated by a control, Inherent Risk / Control level values are displayed when available.

) The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact of this risk.

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

Trend Analysis

This report presents:

- the net risk average over the last three years
- the net risk projection for the coming year.

Access path

Analysis > Risks > Effectiveness > 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 catastrophe	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	↘
⚠ Damage to physical assets	High	High		→	No	High	→

Result calculation

Calculation method

Risk Forecast = Net Risk Year N + ((Net Risk Year N – Net Risk Year N-2)/2)

Internal values

Risk rating	Internal value
Very low	1
Low	16
Medium	81
High	256
Very High	625

Example

Risk Forecast = High + ((High – Very High)/2)

Risk Forecast = 256 + ((256 – 625)/2)

Risk Forecast = 71.5 (rounded up to the nearest threshold= 81)

Risk Forecast = Medium

A stylized, light blue globe with a white outline, centered on the Atlantic Ocean. The continents are represented by white shapes. The text "HOPEX LDC" is overlaid in the center of the globe.

HOPEX LDC

CONTENTS



Contents	1
---------------------------	----------

Collecting Incidents	3
---------------------------------------	----------

Connection Profiles to HOPEX LDC	4
---	----------

Managing Incidents with HOPEX IRM	5
--	----------

<i>Accessing incidents</i>	5
--------------------------------------	---

<i>Creating incidents</i>	5
-------------------------------------	---

Specifying incident characteristics	6
--	----------

Recording Incident-Linked Amounts	7
--	----------

Accessing Incident Financial Analysis	7
---	---

Entering a Loss	7
---------------------------	---

Defining scope of a loss	8
------------------------------------	---

Entering Gains	9
--------------------------	---

Recording Recoveries	10
--------------------------------	----

Recording Provisions	10
--------------------------------	----

Viewing Incident-Linked Amounts	10
---	----

Accessing the Incident Library	12
---	-----------

<i>Viewing all incidents</i>	12
--	----

<i>Viewing incidents by materialized risk</i>	12
---	----

<i>Viewing incidents by risk type</i>	12
---	----

<i>Viewing incidents by affected element</i>	12
--	----

<i>Viewing incidents with a possible impact</i>	13
---	----

Analyzing Incidents	14
--------------------------------------	-----------

Incident Qualitative Analysis	14
---	----

<i>Risks and controls</i>	14
-------------------------------------	----

<i>Risk factors</i>	15
-------------------------------	----

<i>Risk consequences</i>	15
------------------------------------	----

Incident Scope	15
--------------------------	----

Impact analysis of Incidents	16
--	----

Managing Macro-Incidents	17
------------------------------------	----

<i>Connecting incidents to macro-incidents</i>	17
--	----

<i>Creating a macro-incident</i>	18
<i>Analyzing macro-incidents</i>	18
Incident Management Process	20
Incident Management Process General Description	20
Incident Management Process Steps	20
<i>Submitting incidents</i>	20
<i>Validating incidents</i>	20
<i>Closing incidents</i>	21
<hr/>	
Reports Related to Incidents	23
Loss Analysis Reports	24
Incident and Loss Distribution	24
<i>Access path</i>	24
<i>Report parameters</i>	24
Incident and Loss Evolution by Month	25
<i>Access path</i>	25
<i>Report parameters</i>	25
Incident and Loss Evolution by Risk Type	26
<i>Access path</i>	26
<i>Report parameters</i>	26
Back Testing Reports	27
Back Testing Matrix	27
<i>Access path</i>	27
<i>Report parameters</i>	27
Back Testing By Risk Type	28
<i>Access path</i>	28
<i>Report parameters</i>	28
Back Testing by Business Line	28
<i>Access path</i>	28
<i>Report parameters</i>	29
Capital Calculation Reports	30
Loss Distribution Matrix	30
<i>Access path</i>	30
<i>Report parameters</i>	30
BIA Approach	31
<i>Access path</i>	31
<i>Report parameters</i>	31
TSA Approach	32
<i>Access path</i>	32
<i>Report parameters</i>	32

COLLECTING INCIDENTS



The incident is the basic element for data collection concerning operational risk.

) *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.*

HOPEX IRM enables you to organize follow-up of incidents and losses, to identify their causes and measure their impacts.

The system manages the complete life cycle of incidents, and you have tracking information available with a detailed history of recordings.

The GRC Manager/Incident and Loss Administrator may want to analyze incidents before validating data. He/she can view results in the form of dynamic reports. He/she may also decide to group incidents to create a macro-incident.

- 6 [Connection Profiles to HOPEX LDC](#)
- 6 [Managing Incidents with HOPEX IRM](#)
- 6 [Specifying incident characteristics](#)
- 6 [Accessing the Incident Library](#)
- 6 [Analyzing Incidents](#)
- 6 [Incident Management Process](#)

- *For more information on how to treat incidents, see the documentation concerning action plans: [Using Action Plans](#).*

CONNECTION PROFILES TO HOPEX LDC

To connect to HOPEX, see **HOPEX Common Features**, "HOPEX desktop", "Accessing HOPEX (Web Front-End)".

Profiles	Desktop	Tasks
Incident and Loss Administrator (or IRM Manager)	HOPEX IRM	<p>Has rights on all objects and workflows. Prepares the work environment and create elements required for management of incidents and losses. Manages:</p> <ul style="list-style-type: none"> - users and assignment of roles. - description of the environment: org-units and organizational processes, regulatory environment, IT resources. <p>Can intervene in:</p> <ul style="list-style-type: none"> - declared incidents - action plans and actions
IRM Contributor	IRM Contributors	<p>Use the simplified HOPEX Explorer desktop.</p> <ul style="list-style-type: none"> - Declare incidents <p>See The IRM Contributor Desktop.</p>

- For more details, see also [Accessing the IRM Manager Desktop](#).

MANAGING INCIDENTS WITH HOPEX IRM

Accessing incidents

To access incidents:

- > (HOPEX IRM desktop), Select **Libraries > Incidents > All Incidents**.
 - See also [Accessing the Incident Library](#).
- > (IRM Contributor profile) Click **Home > My Incidents**.

Creating incidents

To create an incident:

1. In the **HOPEX IRM** desktop, select **Libraries > Incident Library > All Incidents**.
2. click **New**.
 - With the "IRM Contributor" profile, click **New Incident** from the Home Page.
3. In the incident property page, enter for example its **Name**.
4. Specify the **Declarant Entity**, which is a required field.
 -) 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.

See also [Specifying incident characteristics](#).

SPECIFYING INCIDENT CHARACTERISTICS

To modify incident characteristics:

1. See [Accessing incidents](#).
The list of incidents you have declared appears in the edit area.
2. In the incident properties, select the **Characteristics** page.
3. The following information can be specified:
 - **Description** is a comment describing the incident.
 - **Declaration Date, Detection Date** and current **Occurrence Date**, which constitute incident key dates.
 - *To specify a date, use the calendar at the right of the field.*
 - *Incident declaration and detection dates can differ, the declaration date being later than the detection date.*
 - **Macro-incident**: to connect the current incident to an existing or new Macro-Incident.
 -) *A macro-incident is an event that impacts more than one business or company of the same group.*
 - *For more details, see [Managing Macro-Incidents](#).*
 - **Near-miss**: check box to be selected if it is a **near-miss** incident.
 -) *A near-miss is an incident that did not result in injury, illness, or damage - but had the potential to do so.*
 - **Nature**: you may enter the financial nature of the incident.
 - **Status**: Indicates current status of the incident in the incident management process.
 - *The **Status** appears grayed since it is managed by the workflow associated with the incident. For more details, see [Incident Management Process](#).*

RECORDING INCIDENT-LINKED AMOUNTS

When the incident has been declared, we can record amounts linked to the incident and its consequences, for example *losses*.

-) *A loss is the negative financial result of an event.*
-) *A gain is the positive financial consequence of an incident.*
-) *A provision is an amount deducted from the result to cover risks or unexpected charges. Several provisions can concern a single risk.*
-) *A recovery is a sum, which in certain circumstances can reduce the amount of losses linked to operational risk. It enables recovery of a proportion of the amounts involved in the incident.*

Accessing Incident Financial Analysis

To access financial analysis data of an incident:

1. See [Accessing incidents](#).
The list of incidents you have declared appears in the edit area.
2. Select the incident you wish to modify.
3. In the incident properties, select the **Financial Analysis** page.
Total amounts appear in the **Total Amounts** section.
 - *For more details on incident total amounts, see [Viewing Incident-Linked Amounts](#).*

Entering a Loss

To enter a *loss*:

-) *A loss is the negative financial result of an event.*
- 1. See [Accessing incidents](#).
- 2. In the incident properties, select the **Financial System** page.
 - *For more details, see [Accessing Incident Financial Analysis](#).*
- 3. Expand the **Losses, Gains, Recoveries and Provisions** section.
- 4. Select the **Losses** tab and click the **New** button.
- 5. Select the new loss and click **Properties**.
- 6. In the **Characteristics** tab, complete the following fields:
 - **Name**
 - **Description**: comment concerning the loss.
 - **Effective Date**
 - **Nature**: "Loss of or damage to assets", "Write downs", "Loss of recourse", "Legal liability", etc.
 - **Account** in which the incident is counted.
 - *For more details on the account concept, see [Control Environment](#).*

7. Fill in the **Amount** field and select another currency if it is different from the default local currency.
 - You may specify your default local currency from the application main menu.
 - Amounts entered in a currency are converted to the local currency and to the central currency. If no exchange rate has been previously defined by the administrator, the amount is automatically taken into account in the central currency.
 - If you are not sure of the amount, you can select the **Amount is Estimated** check box. The amount entered will not be included in **Gross actual losses** related to the incident.
 - Losses relating to a near-miss are generally estimated. However you can enter real losses.
8. Expand the **Scope** section and, if required, enter information specific to the loss, for example:
 - **Entity** against which this loss must be accounted.
By default, this is the same entity as that declared for the incident.
 - **Business Line** concerned by the loss.
 - For more details on elements defining scope of an incident or loss, see [Defining scope of a loss](#).
9. Click **OK**.

Defining scope of a loss

Scope of a loss enables definition of location of the loss, the associated incident and therefore a risk within the organization.

- Organization description is detailed in chapter [Managing your IRM Environment](#).

The scope is specified on several component types:

- **entities** concerned by the loss
 -) 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.
- **business lines** concerned by the loss
 -) A business line is a skill or grouping of skills of interest for the enterprise. It corresponds for example to major product segments, to distribution channels or to business activities.
- **risk types** to be associated with the loss
 -) A risk type defines a risk typology standardized within the context of an organization.
- **business processes** and **organizational processes** concerned by the loss
 -) A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real

implementation of the business process in the organization. A business process can also be detailed by a functional view.

) An organizational process describes how to implement all or part of the process required to make a product or handle a flow.

- **products** impacted by the loss
 -) A product represents commodities offered for sale, either goods or merchandise produced as the result of manufacturing, or a service, ie. work done by one person or group that benefits another.
- **applications** impacted by the loss
 -) An application is a set of software tools coherent from a software development viewpoint.
- **requirements** expected related to loss management
 -) 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.

Entering Gains

) A gain is the positive financial consequence of an incident.

To enter a gain:

1. See [Accessing incidents](#).
2. In the incident properties, select the **Financial System** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Gains** tab and click the **New** button.
The new gain appears in the list.
5. Select the new gain and click **Properties**.
The properties dialog box opens.
6. In the **Characteristics** tab, complete the following fields:
 - **Name**
 - **Description**: comment concerning the loss.
 - **Effective Date**
 - **Account** in which the incident is counted.
 - For more details on the account concept, see [Regulatory Environment](#).
7. Expand the **Amount** section and, if required, enter information concerning the loss amount.
 - Amounts entered in a currency are converted to the local currency and to the central currency.
 - If no exchange rate has been previously defined by the administrator, the amount is automatically taken into account in the central currency.
 - If you are not sure of the amount, you can select the **Amount is Estimated** check box. The amount entered will not be included in totals related to the incident.
 - Losses relating to a near-miss are generally estimated. It is however possible to enter actual gains.

8. Expand the **Scope** section and, if required, enter information specific to the gain.
 - For more details on elements defining scope of an incident, see [Defining scope of a loss](#).
9. Click **OK**.

Recording Recoveries

) A recovery is a sum, which in certain circumstances can reduce the amount of losses linked to operational risk. It enables recovery of a proportion of the amounts involved in the incident.

It is useful to differentiate between **recoveries** from insurance and those from other areas such as litigation, third-parties, etc.

To enter a recovery:

1. See [Accessing incidents](#).
2. In the incident properties, select the **Financial System** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Recoveries** tab and click the **New** button.
The new recovery appears in the list.
5. To specify information specific to a recovery, proceed in the same way as for a gain.
 - For more details, see [Entering Gains](#).

Recording Provisions

) A provision is an amount deducted from the result to cover risks or unexpected charges. Several provisions can concern a single risk.

To enter a **provision**:

1. See [Accessing incidents](#).
2. In the incident properties, select the **Financial System** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Provision** tab and click the **New** button.
The new provision appears in the list.
5. To specify information specific to a provision, proceed in the same way as for a gain.
 - For more details, see [Entering Gains](#).

Viewing Incident-Linked Amounts

To view Incident-related Amounts:

1. See [Accessing incidents](#).
2. In the incident properties, select the **Financial System** page.

The **Total Amounts** section automatically calculates the sum of all incident-related financial elements (losses, gains, recoveries and provisions).

If an element is **Estimated**, it is not included in the losses total.

Amounts appear in the central currency and in the local currency.

Total Amounts		
Gross Loss:	0.00 €	Gross Loss (local):
Gross Actual Loss:	0.00 €	Gross Actual Loss (local):
Recoveries:	0.00 €	Recoveries (local):
Net Loss:	0.00 €	Net Loss (local):
Net Actual Loss:	0.00 €	Net Actual Loss (local):

The following fields give valuated indications on incidents:

- **Gross Loss**
Sum of losses related to the incident (including estimated losses).- Gains
- **Gross actual loss**
Gross Actual Loss = Sum of losses related to the incident without estimated losses .- Gains.
- **Recoveries**
Sum of insurance and non-insurance recoveries
- **Net Loss**
Net Loss = Gross Loss - Recoveries
- **Net Actual Loss**
Net Actual Loss = Gross Actual Loss - Recoveries

ACCESSING THE INCIDENT LIBRARY

You can manage incidents directly from the Incident Library.

To access them:

- > (**HOPEX IRM** desktop), Select **Libraries > Incidents**.

Tiles and lists within each tile enable you to access incidents according to different criteria.

Viewing all incidents

Libraries > Incidents > All Incidents

This tile enables you to view all incidents:

- Macro Incidents
 -) *A macro-incident is an event that impacts more than one business or company of the same group.*
- Incidents to Review
 - *This list displays incidents which have been declared et which must be validated. For more details, see [Validating incidents](#).*
- Open Incidents
 - *This list displays the incidents you can close. For more details, see [Closing incidents](#).*
- High Impact Incidents
 - *This list displays all Incidents with High Impact.*

Viewing incidents by materialized risk

Libraries > Incidents > By Risk

Displays all incidents by risk and contains two lists:

- Incidents with materialized Risks
- Incidents without materialized Risks

Viewing incidents by risk type

Libraries > Incidents > By Risk Taxonomy

This list displays all incidents in your environment in a tree structured around Risk Types.

Viewing incidents by affected element

Libraries > Incidents > By Affected Elements

Various lists enable you to view objects on which incidents had a high impact.

- Incidents by business line
- Incidents by application
- Incidents by entity
- Incidents by process
- Incidents without affected elements

Viewing incidents with a possible impact

Libraries > Incidents > By Impact

This tile displays incidents in your environment:

- which may impact compliance of your organization with regulatory requirements,
- which materialize key risks.

Drop-down lists enables you to access incidents according to:

- regulatory impact
- risk causality
 - *Incidents against risks which may cause other risks are shown here.*

ANALYZING INCIDENTS

When basic characteristics of the incident have been specified, you can enter advanced characteristics in the context of incident analysis.

This work consists of linking the incident to the environment defined by your organization.

- For more details on environment components, see [Managing your IRM Environment](#).

Incident Qualitative Analysis

To access incident qualitative analysis:

1. See [Accessing incidents](#).
2. Open the properties of the incident.
3. In the **Characteristics** tab, expand the **Qualitative Analysis** section.

Risks and controls

Associating an incident to a *risk* and to a *control* is an essential step in managing incidents.

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

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

To do this:

1. In the incident properties, select the **Characteristics** page.
2. Expand the **Qualitative Analysis** section.
3. Click the arrow at the right of the **Materialized Risk** field and select **Link Risk**.
The list of risks defined in your repository appears.
4. Select the risk that interests you and click **OK**.
The incident is now attached to the risk.
5. Specify the **Impact** characterizing impact of the incident on environment elements.
 - "Very High"
 - "High"
 - "Medium"
 - "Low"
 - "Very Low"
6. Specify the **Priority** characterizing the incident relative importance.
 - "High"
 - "Medium"
 - "Low"

7. Click the arrow at the right of the **Control** field and select **Link Controls**.
The list of controls defined in your repository appears.
8. Select the control that interests you and click **OK**.
The incident is now attached to the control.

Risk factors

Many *risk factors* are defined within the framework of international, national or inter-professional regulations, or within the enterprise itself.

) *A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several Risks can originate from a same Risk Factor Examples: the use of a hazardous chemical product, the complexity of an application, the size of a project, the number of involved parties, the use of a new technology, the lack of quality assurance, the lack of rigor in requirements definition...*

With each risk, you can associate one or more *risk factors*, sources of risks that have intrinsic potential to endanger organization operation. For example, dangerous chemical products, competitors, governments, etc.

To define risk factors associated with an incident:

1. In the incident properties, select the **Characteristics** page.
2. Expand the **Qualitative Analysis** section.
3. Select the **Risk Factor** tab and click the **Connect** button.
The list of risk factors defined in your repository opens.
4. Select the risk factor associated with the incident.
5. Click **OK**.
The risk factor appears in the list.

Risk consequences

) *A risk consequence can be positive or negative. It is associated with a type, which enables its characterization, for example: image, environment, employees.*

To define risk consequences associated with an incident:

1. In the incident properties, select the **Characteristics** page.
2. Expand the **Qualitative Analysis** section.
3. Select the **Risk Consequence** tab and click the **Connect** button.
The list of risk consequences defined in your repository opens.
4. Select the risk consequences associated with the incident.
5. Click **OK**.
The risk consequence appears in the list.

Incident Scope

To specify the scope of an incident:

1. See [Accessing incidents](#).
2. In the incident properties, select the **Characteristics** page.
3. Expand the **Scope** section.

Incident scope enables definition of risk location within the organization.

- *Organization description is detailed in paragraph [Organization](#).*

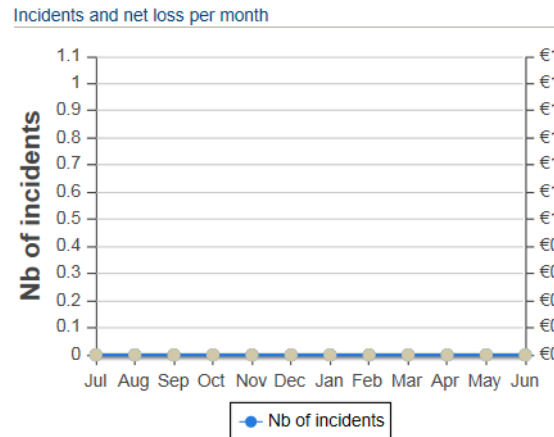
The scope is specified on several component types:

- **entities** concerned by the incident
 -) *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.*
- **business lines** concerned by the incident
 -) *A business line is a skill or grouping of skills of interest for the enterprise. It corresponds for example to major product segments, to distribution channels or to business activities.*
- **risk types** to be associated with the incident
 -) *A risk type defines a risk typology standardized within the context of an organization.*
- **business processes** and **organizational processes** concerned by the incident
 -) *A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.*
 -) *An organizational process describes how to implement all or part of the process required to make a product or handle a flow.*
- **products** impacted by the incident
 -) *A product represents commodities offered for sale, either goods or merchandise produced as the result of manufacturing, or a service, ie. work done by one person or group that benefits another.*
- **applications** impacted by the incident
 -) *An application is a set of software tools coherent from a software development viewpoint.*
- **requirements** expected related to incident management
 -) *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.*

Impact analysis of Incidents

HOPEX IRM offers the possibility to analyse, from several perspectives, the distribution of incidents linked to the environment.

For more information, see [Loss Analysis Reports](#).



Managing Macro-Incidents

An incident concerns only one business line and one organizational unit, which is why **HOPEX IRM** enables creation of macro-incidents.

The *macro-incident* enables representation of a group of incidents that have generated losses on different business lines and/or different companies of the group.

) *A macro-incident is an event that impacts more than one business or company of the same group.*

For example, a wilful incident in a building can have repercussions on several business lines or organizational units of the group.

Connecting incidents to macro-incidents

You can connect incidents to macro-incidents in two ways:

- from the properties of a macro-incident, in the **Incidents** tab, by connecting existing incidents
- from an incident (operation described below)

To connect an incident to the macro-incident:

1. See [Accessing incidents](#).
2. Select the incident you want to modify and click **Properties**.
3. Select the **Characteristics** tab.
4. Click the arrow at the right of the **Macro-Incident** field and select **Link Macro Incidents**.
The list of macro-incidents appears.
5. Select the macro-incident that interests you and click **OK**.
The incident is now attached to the macro-incident.

- *Incidents are visible in the **Incidents** tab of the macro-incident.*

Creating a macro-incident

- This feature is proposed only to Risk Managers and Incidents and Losses Administrators.

To create a macro incident:

1. Select **Libraries > Incident Library > All Incidents**.
2. From the drop-down list, select **Macro-Incidents**.
The list of macro-incidents you have declared appears in the edit area.
3. click **New**.
The new macro-incident appears in the list.
4. In the macro-incident properties, select the **Characteristics** page.
5. Specify the following fields:
 - **Name**
 - **Description**: comment concerning the macro-incident.
6. Expand the **Scope** section and, if required, enter information specific to the macro-incident.
 - For more details on elements defining scope, see [Defining scope of a loss](#).

Analyzing macro-incidents

Incidents connected to the macro-incident

To access the list of incidents connected to a macro-incident:

- › In macro-incident properties, select the **Incidents** page.
 - In the **Incidents** page of the macro-incident, the fields **Number of Validated Incidents**, **Date of First Occurrence** and **Date of Last Occurrence** are completed automatically.

Macro-incident amounts

The **Total Amounts** section of the macro-incident properties presents the sum of all financial elements specified for incidents connected to the macro-incident.

The following fields are calculated automatically:

- **Gross Loss**
Sum of losses related to the incident (including estimated losses).- Gains
- **Gross actual loss**
Gross Actual Loss = Sum of losses related to the incident without estimated losses .- Gains.
- **Recoveries**
Sum of insurance and non-insurance recoveries
- **Net Loss**
Net Loss = Gross Loss - Recoveries
- **Net Actual Loss**
Net Actual Loss = Gross Actual Loss - Recoveries

Losses evolution report

This report presents evolution of net losses per month of incidents connected to the macro-incident.

To access the Reports tab:

- In macro-incident properties, select the **Loss Evolution** page.

INCIDENT MANAGEMENT PROCESS

Incident Management Process General Description

Incident management process steps are as follows:

- Having specified characteristics of a new incident, the incident declarant should **Submit** the incident.
 - The Risk Manager can:
 - **Validate** the incident, which takes status "Validated".
 - **Reject** the incident.
 - When a validated incident is considered as terminated, the Risk Manager can:
 - **Close** the incident, which takes status "Closed".
 - See [Incident Workflow](#) for the corresponding workflow definition diagram.
-

Incident Management Process Steps

Submitting incidents

When you have specified information concerning the incident, you can submit.

To submit an incident:

1. See [Accessing incidents](#).
2. Right-click the incident you want to submit and select **Incident Declaration > Submit for Validation**.
The incident takes status "To Be Validated" and appears in the list of incidents to be validated by the Risk Manager.

Validating incidents

When incidents have been specified with their losses, recoveries and provisions, you can then make use of your data.

- *Only Risk Managers are authorized to validate incidents.*

To validate an incident:

1. Select **Libraries > Incidents > All Incidents**.
2. In the drop-down list select **Incidents to Review**.
 - *You can also access the incidents to Review from **My tasks > Review > Incidents to review**.*

The list of incidents for which you are responsible appears in the edit area.

3. Right-click the incident that interests you and select one of the following commands:
 - **Validate** the incident, which takes status "Validated".
 - **Reject** the incident.

Closing incidents

When the incident has been validated, the Risk Manager can decide that this incident will not be modified further, and therefore close it .

- *Only Risk Managers are authorized to validate incidents.*

To do this:

1. Select **Libraries > Incidents > All Incidents**.
2. In the drop-down list select **Open incidents**.
3. Right-click the incident you want to close and select **Close**.

REPORTS RELATED TO INCIDENTS



The different report templates proposed as standard by **HOPEX LDC** enable analysis and follow-up of incidents and their financial consequences. Reports are presented in the local currency of the user if the exchange rate between reference currency and local currency is specified. If the exchange rate is not specified, reports are presented in the reference currency.

- For more details on the use of reports, see the **HOPEX Common Features** guide.

- 6 [Loss Analysis Reports.](#)
- 6 [Back Testing Reports.](#)
- 6 [Capital Calculation Reports.](#)

LOSS ANALYSIS REPORTS

Incident and Loss Distribution

This report displays distribution of incidents and losses selected according to different perspectives: by entity, by business line, by risk type or by process.

- For more details on the procedure that enables connection of the incident or loss to an entity or process, see [Defining scope of a loss](#).

Access path

Analysis > Incidents > Losses > Incident & Loss Breakdown

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Organizational Process	Organizational Process	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Business processes	Business processes	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Entities	Entity	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Incident and Loss Evolution by Month

This report displays monthly distribution of incidents and monthly distribution of losses on two different diagrams.

- For more details on how to connect an incident to a loss, see [Entering a Loss](#).

Access path

Analysis > Incidents > Losses > Incident & Loss Evolution per Month

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Organizational Process	Organizational Process	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Business processes	Business processes	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Entities	Entity	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Results

This report displays the number of incidents and the corresponding net loss (sum of losses - sum of recoveries) per month between two dates.

- *If no parameter is defined, all incidents are taken into account. Otherwise, only the incidents connected to the objects specified as a parameter and their children (risk types, business processes, organizational processes, entities and business lines) are displayed.*

Incident and Loss Evolution by Risk Type

This report displays monthly evolution curves of incidents and losses in the same diagram.

- *For more details on how to connect an incident to a loss, see [Entering a Loss](#).*

Access path

Analysis > Incidents > Losses > Incident & Loss Evolution per Risk Type

Report parameters

This report consists in selecting incidents and losses that will be presented while specifying the risk types in their their scope.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. The user currency is used by default.
Warning threshold	Real	Takes into account the incidents whose loss amount is higher than this threshold.
Begin Date	Date	One year before the current date (by default)
End date	Date	Current date (by default)
Risk Type	Risk Type	Selection of incidents connected to risk types of the list or to their subtypes. Not mandatory.

Results

This report consists of two parts:

- **Incident evolution** per month and risk type: displays the number of incidents declared per month between a defined start date and end date, and distributed by risk type.
- **Loss evolution** per month and risk type: displays the net loss (sum of losses - sum of recoveries) of a set of incidents.
 - *For these two report chapters, if no risk type is defined as a parameter, all incidents are taken into account. Otherwise, only the incidents connected to the selected risk types and their children are displayed.*

BACK TESTING REPORTS

These reports indicate financial losses of risks studied from their attached incidents.

- For more details on the procedure that enables connection of an incident or loss to a risk type, see [Defining scope of a loss](#).

Risks displayed in reports are the risks defined in parameters and their sub-risks.

Back Testing Matrix

Access path

Analysis > Incidents > Back Testing > Back Testing Matrix

Report parameters

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

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Organizational Process	Organizational Process	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Business processes	Business processes	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Entities	Entity	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Back Testing By Risk Type

Access path

Analysis > Incidents > Back Testing By Risk Type

Report parameters

This consists of selecting risk types that will be presented in the report.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.

Back Testing by Business Line

This consists of selecting business lines that will be presented in the report.

Access path

Analysis > Incidents > Back Testing By Business Line

Report parameters

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

CAPITAL CALCULATION REPORTS

These reports are used to evaluate amount of capital to be provided to cover operational risks.

Loss Distribution Matrix

This report indicates distribution of losses as a function of business lines (presented in columns) and risk types (presented in rows).

For each pair (business line, risk type), this report presents:

- The total amount of losses,
- The minimum amount of losses,
- The maximum amount of losses,
- The number of incidents.

Access path

Analysis > Incidents > Capital Calculation > Loss Distribution Matrix

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Net loss threshold	Real	Minimum amount of displayed losses.
Analysis year	Short	Year preceding current year by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

BIA Approach

This report gives an estimate of capital amount to be allocated for a business line. For each year of the period defined by parameters, the report presents:

- The total of gross revenues, by year
 - To create revenues, see [Entering gross revenues for incident management](#).
- The average gross revenue over the number of years specified as parameter
- The BIA defined as parameter
- The capital amount to be allocated for the business line (percentage of BIA applied to average gross revenue).

Access path

Analysis > Incidents > Capital Calculation > BIA Approach.

Report parameters

This consists of selecting incidents and losses that will be presented in specifying elements that define their scope. In this report, the scope is defined by a single business line.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Gross revenue threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Average period	Short	Number of years to which average calculation relates.
Percentage of BIA	Real	Percentage value to be applied.
Business line	Business line	Mandatory.

TSA Approach

This report, derived from Basel II, gives an estimate of capital amount to be allocated by business line.

For each business line, the report presents:

- The total of gross revenues, by year
- The average gross revenue over the number of years specified as parameter
- The TSA rate adopted for the business line
- The capital amount to be allocated for the business line (percentage of TSA applied to average gross revenue).

Access path

Analysis > Incidents > Capital Calculation > BSA Approach.

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Gross revenue threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Average period	Short	Number of years to which average calculation relates.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

