

HOPEX IRM

HOPEX V5



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 - 2021

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



HOPEX IRM Common Features

User Guide

HOPEX V5



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 is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2021

All rights reserved.

HOPEX is a registered trademark of MEGA International.

Windows is a registered trademark of Microsoft Corporation.

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

CONTENTS



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

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

Accessing the IRM Manager Desktop	11
<i>Profiles used in IRM solutions</i>	11
<i>IRM Profiles/Solutions Summary</i>	13
The IRM Documentation	14

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

Reusing Regulation Data	16
<i>Converting regulation data</i>	16

Managing Teams	18
<i>Creating controllers</i>	18
<i>Creating skill types</i>	18
<i>Creating skills</i>	18
<i>Creating skill levels</i>	18
<i>Viewing user skills</i>	19

Managing Currencies	20
<i>Defining Central Currency</i>	20
<i>Defining local currencies available to users</i>	20
<i>Specifying your local currency</i>	21
<i>Managing Exchange Rates</i>	21

Configuring Time Sheets	23
--	-----------

Managing Campaign Calendars	24
<i>Creating schedules</i>	24
<i>Creating calendar periods</i>	24
<i>Connecting a calendar to an audit or test plan</i>	24

Managing Steering Calendars	25
Administering Key Indicators	26
Accessing Indicator Administration Features	26
Defining Indicator Categories	26
Defining Indicator Interpretation logics	27
Defining Indicator Statuses	28
<i>Creating indicator statuses</i>	28
<i>Computation of indicator statuses</i>	28
Defining Aggregation Periods and Methods.	31
<i>Aggregation periods</i>	31
<i>Aggregation methods</i>	32
<i>Creating aggregation periods or methods</i>	32
Defining Key Indicator Value Computation Logics	32
<i>Creating a computation logic</i>	32
<i>Computation logic via query</i>	32
Exporting and Importing IRM Objects	34
Exporting IRM Objects	34
<i>Using the export wizard from the main menu.</i>	34
<i>Exporting IRM objects from a list</i>	34
Importing IRM Objects	35
<hr/>	
Managing your IRM Environment	37
Organization	38
Managing Entities	38
<i>Accessing organization entities.</i>	38
<i>Creating an entity.</i>	38
<i>Creating a sub- entity.</i>	38
<i>Defining entity general characteristics.</i>	39
<i>Specifying responsibilities within an entity.</i>	39
<i>Scoping an entity</i>	40
Managing Processes	41
<i>Accessing processes</i>	41
<i>Process hierarchy</i>	41
<i>Specifying process characteristics.</i>	42
<i>Specifying process scope.</i>	42
<i>Specifying process responsibilities</i>	42
<i>Specifying sub-processes.</i>	43
<i>Managing business continuity.</i>	43
<i>Other sections of a process</i>	44
Managing Business Lines	44
<i>Accessing Business Lines.</i>	44
<i>Connecting entities and processes to a business line.</i>	44
<i>Defining risks and incidents that impact a business line</i>	45
<i>Entering gross revenues for incident management</i>	45
Managing Applications	45
<i>Accessing applications.</i>	45
<i>Specifying application scope</i>	45

Financial Environment	46
Accounts	46
<i>Characteristics of an account.</i>	46
<i>Connecting controls to an account</i>	46
Products	47
Gross Incomes	47
Strategic Environment	48
Risk Environment	49
Describing Risk Environment	49
Defining the Environment of a Specific Risk	49
Risk types	50
<i>Creating a risk type</i>	50
<i>Analyzing the impacts of a risk type.</i>	50
Risk Factors	51
Risk consequences	51
Control Environment.	52
The Compliance Environment.	53
Managing your Regulatory Environment	53
<i>Using UCF Import</i>	53
<i>Creating Regulatory Content Manually</i>	55
Managing Business Policies	56
<i>Creating business policies.</i>	56
Defining Applicable Regulations and Business Policies.	56
<i>Regulatory content applicability.</i>	56
<i>Reviewing regulatory frameworks after UCF import</i>	56
<i>Selecting the regulatory content applicable to your organization</i>	57
Defining the Scope of Regulations and Business Policies	57
Responsibilities (RACI)	58
<i>Responsibility levels.</i>	58
<i>Specifying Responsibilities</i>	58
 Managing Key Indicators	 59
Accessing Key Indicators	60
Defining Key Indicators	61
Creating a Key Indicator	61
Specifying the Aggregation Period and Method	61
Example of a Key Indicator	62
About Key Indicator Categories	64
Description of Key Indicator Categories	64
Relation between Indicator Category and Interpretation Logic	64
More Key Indicator Characteristics	66
Editing Key Indicator Parameters	66
Defining a Measurement Unit to be Displayed in Reports	67
Activating / Deactivating a Key Indicator	67
Specifying the Indicator Scope	67
Specifying Action Plans	68
Connecting Risks	68

Consulting the Key Indicator Dashboard	69
Indicator Status	69
<i>Default statuses</i>	69
<i>Information about indicator status computation</i>	69
Time to Failure	70
Last Measurement of the Key Indicator	70
Key Indicator Value	70
Defining Measurement Frequency and Notifications	71
Specifying Measurement Frequency	71
Managing Notifications	71
Entering Periodic Key Indicator Values	71
<i>Entering a key indicator value manually</i>	72
<i>Parameterizing automatic value entering</i>	72
Viewing the Indicator Graph	73
<hr/>	
Managing Assessment Campaigns	75
Accessing Assessments by Profiles	76
Accessing Assessment Templates	77
Preparing the Assessment Environment	78
Prerequisites to Risk Assessment	78
Pre-requisites to Control Assessment	78
Starting an Assessment Campaign	79
Creating Assessment Campaigns	79
Creating an Assessment Session Manually	81
Completing Questionnaires	83
Following up assessments progress	84
<i>Consulting Session Results</i>	84
<i>Viewing assessment campaign results</i>	84
<i>Validating Assessment Questionnaires</i>	84
<i>Asking a respondent to modify answers</i>	84
<i>Viewing assessment campaign reports</i>	85
<i>Reassigning questionnaires</i>	85
Consulting Assessment Results	85
<hr/>	
IRM Reports	105
IRM Report Availability	106
Key Indicator Reports	107
Indicator Comparator	107
Multi-Gauge chart	108
Multi-line chart	109
Action Plan Follow-up Reports	111
Action Plan Follow-Up	111
Access path	111

Result	111
Gantt report	112

IRM Solution Workflows.....115

Risk Workflows.....	116
Testing Workflows	117
Test Plan/Audit Plan Workflow	117
Test Workflow	118
Test Activity Workflow	119
Expense Sheet Workflow	120
Action Plan Workflows	121
"Bottom-up" Action Plan Workflow	121
"Top-down" Action Plan Workflow	122
Action Workflow	123
Incident Workflow	124
Campaign Workflow	125
Assessment Campaign Workflow	125
Execution (Automatic) Campaign Workflow	125

The IRM Contributor Desktop.....127

Presentation of the IRM Contributor Desktop	128
Accessing the IRM Contributor Desktop	128
Features Available to the IRM Contributor	129
Home Page	130
Dashboard	130
My Tasks	130
Environment	131
Risks	131
Controls	131
Incidents	131
Viewing your Environment	133
Business and organizational processes	133
Applications	133
Business lines	133
Entities	133
Dashboard and Widgets	134
Widgets for Action Plans	134
Widgets specific to IRM	134
Widgets specific HOPEX Internal Audit	135
Managing Incidents	136
Creating incidents	136
Accessing incidents	136

Managing Action Plans and Actions	137
<i>Context for action plan creation</i>	137
<i>Accessing action plans</i>	137
<i>Connecting an issue to an action plan</i>	137
<i>Indicating action plan progress</i>	137
<i>Managing actions</i>	138
Managing Recommendations	139
<i>Accessing recommendations</i>	139
<i>Implementing recommendations</i>	139
<i>Viewing recommendation widgets</i>	140
Managing Questionnaires and Check-lists	141
<i>Accessing Questionnaires</i>	141
<i>Answering a Questionnaire</i>	141
<i>Completing Assessment Check-lists</i>	142
Creating Risks and Controls	143
<i>Creating risks</i>	143
<i>Creating controls</i>	143
Managing Key Indicators	144
<i>Accessing Key Indicators</i>	144
<i>Enter a key indicator value</i>	144
<i>Submitting an action plan on a key indicator</i>	144
Performing a BIA (Business Impact Analysis)	146
Taking Part in Business Continuity Plans	147
<i>Viewing BCPs tested by ongoing exercises</i>	147
<i>Viewing BCPs triggered by ongoing crises</i>	147

Appendix - Computation Rules. 149

Risk Control Level	149
<i>Context</i>	149
<i>Computation method</i>	149
<i>Computation example</i>	150
Inherent risk	150
<i>Computation method</i>	150
<i>Possible values</i>	151
Residual Risk	151
<i>Computation method</i>	151
<i>Possible values</i>	152
RTO (Recovery Time Objective) Computation	152
Business Impact Computation	153

IRM Glossary 155

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.

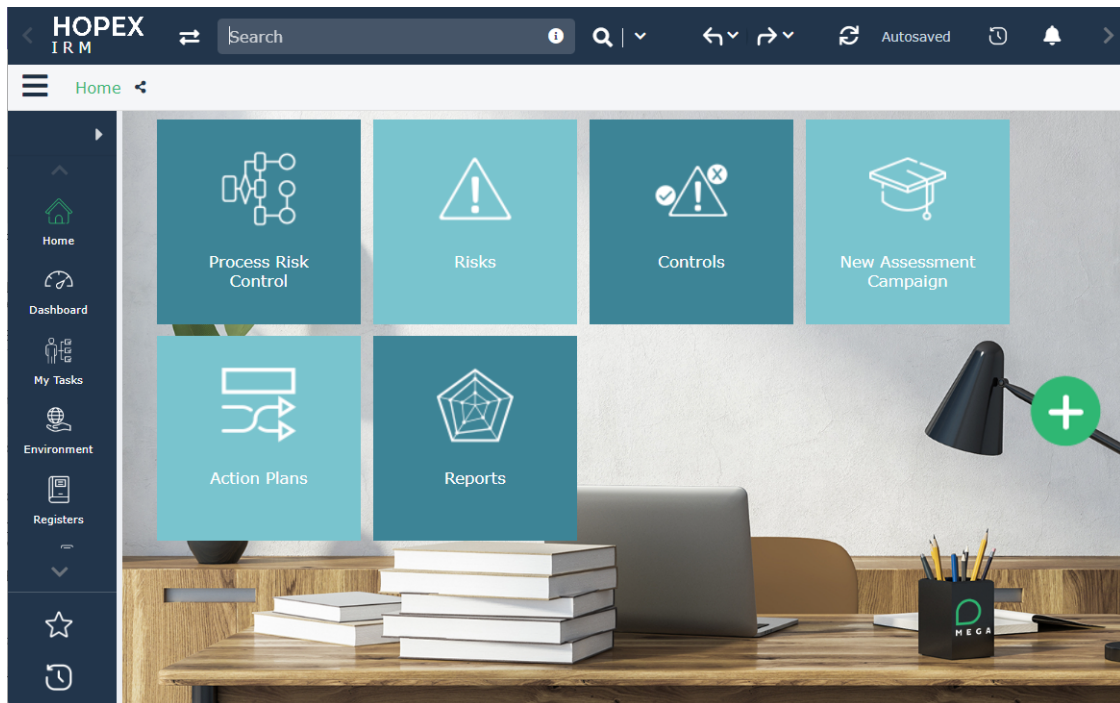
It is available with the following solutions:

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

➤ *For more details on **HOPEX Internal Audit** see the corresponding documentation.*

- **HOPEX BCM**

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



Home page tiles

The home page contains shortcuts to the most useful object lists and features.

For example, the “Process Risk Control” tile enables you to access risks and controls via trees of business and organizational processes.

You can add tiles that correspond to different IRM-related topics:

- Environment
- Risks
- Controls
- Campaigns
- Incidents
- Audit
- Action plans
- Business continuity

🖱️ To add tiles, see [Customizing the Home Page of your Desktop](#).

Dashboard

This navigation pane 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
- **Business Continuity**: displays the Business Impact Analyses (BIAs), exercises and crises I need to handle.
 - ☛ For more information on business continuity, see **HOPEX BCM** documentation.
- **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**
 - ☛ The objects to review are the objects which need to be validated.
 - Incidents to Review
 - ☛ See [Validating incidents](#).
 - Risks to Review
 - ☛ See [Validating or rejecting a risk](#).
 - Vacation Requests to Review
 - Expenses to Review
- **Audit**
 - Work program (individual work program and audit global work program)
 - Past audits
 - ☛ This menu applies to **HOPEX Internal Audit** only. For more details, see [Introduction to HOPEX Internal Audit](#).
 - **Testing** (controls)
 - Activities
 - Vacation Requests
 - Time sheets
 - Expenses
 - ☛ This menu applies to **HOPEX Internal Control** only. For more details, see [Control Testing](#).
- **Time and Expense Management**
 - My Vacation Requests
 - My Timesheets
 - My Expenses
- **Issues**
 - Actions to implement
 - Action plans to implement
 - Recommendations to implement
 - Late Recommendations Only (applies to **HOPEX Internal Audit**)

Environment

See [Managing your IRM Environment](#).

Registers

See:

- [Managing Risks](#)
- [Managing Controls](#)
- [Managing Compliance](#)
- [Managing Key Indicators](#)
- [Collecting Incidents](#)

Assessment

See [Managing Assessment Campaigns](#).

See also the documentation specific to each solution:

- [Assessing Risks](#)
- [Assessing controls](#)

Execution

See [Executing Controls](#).

☞ This navigation pane applies to **HOPEX Internal Control** only.

Business continuity

See [Introduction to HOPEX BCM](#).

☞ This navigation pane applies to **HOPEX BCM** only.

Audit

See [Introduction to HOPEX Internal Audit](#).

☞ This navigation pane applies to **HOPEX Internal Audit** only.

Testing

See [Control Testing](#).

☞ This navigation pane applies to **HOPEX Internal Control** only.

Analysis

See [IRM Reports](#).

ACCESSING THE IRM MANAGER DESKTOP

To connect to **HOPEX**, see [Connecting to HOPEX](#).

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](#) (HOPEX Enterprise Risk Management).

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](#) (HOPEX Internal Control).

Incident and Loss Manager

The incident and loss manager creates elements required for management of incidents and losses.

He manages the description of the environment: entities and organizational processes, regulatory environment, IT resources.

He can deal with:

- 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**
- **HOPEX BCM**

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

- Risk Manager
- Internal Control Director
- Incident and Loss Manager
- 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 Contributor

The contributor performs his/her tasks in a simplified desktop. For more details, see [About the IRM Manager Desktop](#).

IRM Profiles/Solutions Summary

<i>Solutions/ Profiles</i>	<i>ERM</i>	<i>IC</i>	<i>LDC</i>	<i>BCM</i>
IRM functional administrator	X	X	X	X
IRM Manager	X	X	X	X
IRM Contributor	X	X	X	X
Risk Manager	X			X
Internal Control Director		X		
Internal Controller		X		
Incident and Loss Manager			X	

THE IRM DOCUMENTATION

The IRM documentation is structured as follows:

Features common to IRM solutions

- [Managing your IRM Environment](#)
- [Managing Key Indicators](#)
- [Managing Assessment Campaigns](#)
- [IRM Reports](#)
 - ☛ *For information on risks/controls/incidents, see:*
 - [Risk-Related Reports.](#)
 - [Reports Related to Controls](#)
 - [Reports Related to Incidents](#)
- [IRM Solution Workflows](#)
- [Appendix - Computation Rules](#)

HOPEX Internal Control

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

HOPEX Enterprise Risk Management

- [Managing Risks](#)
- [Assessing Risks](#)
- [Risk-Related Reports](#)

HOPEX LDC

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

HOPEX BCM

- [Managing BCM Systems](#)
- [Defining a Business Impact Analysis](#)
- [Designing a Business Continuity Plan](#)
- [Testing a Business Continuity Plan](#)
- [Managing Crises](#)

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.

- ✓ [Reusing Regulation Data](#)
- ✓ [Managing Teams](#)
- ✓ [Managing Currencies](#)
- ✓ [Configuring Time Sheets](#)
- ✓ [Managing Campaign Calendars](#)
- ✓ [Managing Steering Calendars](#)
- ✓ [Administrating Key Indicators](#)
- ✓ [Exporting and Importing IRM Objects](#)

REUSING REGULATION DATA

If your repository contains regulation frameworks or requirements, you need to convert them to be able to reuse them in **HOPEX IRM**.



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.



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.

Source object type	Object type obtained after conversion
Regulation Framework	Regulatory framework
Requirement	Article + Control directive



For more details on regulatory frameworks, see [Managing the Compliance Register](#).

Converting regulation data

To convert regulation frameworks and requirements:

1. From the navigation menu, select **Administration > Tools > Regulation Data Conversion**.

Gauges indicate the percentage of regulation frameworks and requirements which have been converted so far.

2. Click **Launch Data Conversion**.
3. In the **Convert into** column, indicate for each regulation framework if you want to:

- convert it into a 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), or standards.

- convert it into a business policy framework



A policy framework consists of a set of business policies. Policy frameworks may contain sections.

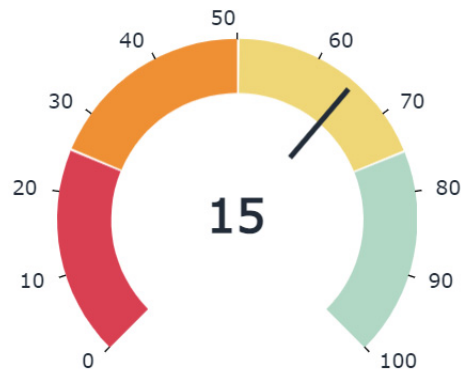
- do not want to convert it



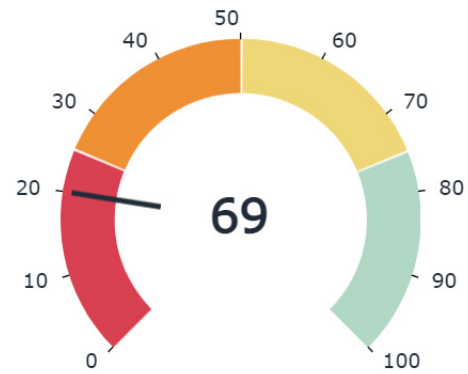
*Regulation Frameworks are by default converted into Regulatory Frameworks. The **Apply Default Conversion Settings** button enables to revert to the initial settings in case you made changes.*

At the end of the conversion, the gauges display an updated percentage.

Converted Regulation Frameworks



Converted Requirements



Converted data can be viewed in the compliance library (**Registers > Compliance**). For more details, see [Managing the Compliance Register](#).

⚠ The regulation framework date is not converted. Moreover, customized characteristics are not converted either.

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.

Viewing user skills

To view the skills of a user:

1. In the navigation menu, select **Administration > Skill Management > All User Skills**.
2. Select a user and click the **Person Skills** button.
The page concerning the user skills is displayed.

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



Central currency is the currency adopted as reference 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.

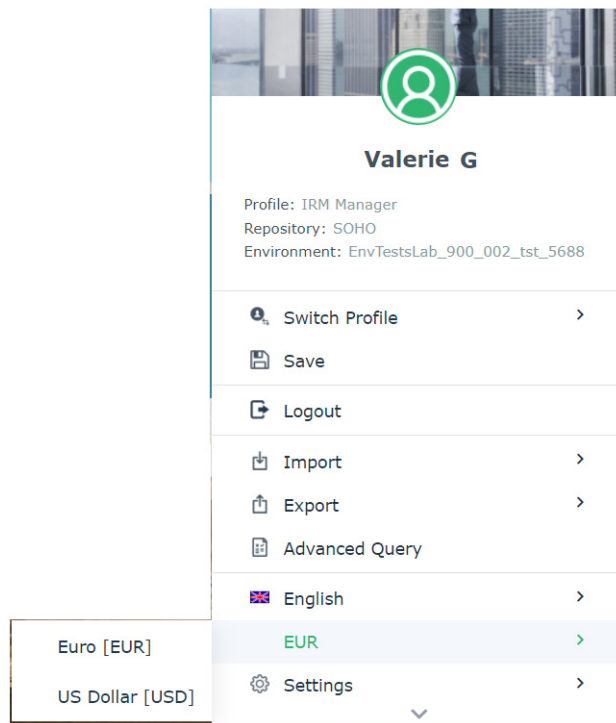
2. In the main menu, select **Settings > Options**.
3. Select the **Installation > Currency** folder.
The list of currencies available as standard appears on the right.
4. Select all the currencies that will be used locally by your users.
5. Click **OK**.

Specifying your local currency

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

To modify your local currency:

1. 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".

MANAGING CAMPAIGN CALENDARS

A calendar is divided into time periods called calendar periods. Calendars can be used in assessment campaigns, in report generation as well as to schedule audits/ 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 schedules

To create a calendar:

1. In the navigation menu, click **Administration > Calendars > 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**.

MANAGING STEERING CALENDARS

Steering calendars are used within the framework of:

- execution campaigns
 - ☛ See [Preparing Control Execution](#).
- action plan reminders

To create and parameterize a steering calendar:

1. In the navigation menu, select **Administration > Calendars > Steering Calendars**.
2. Click **New**.
3. In the wizard that appears, select the context in which you want to use the steering calendar:
 - Control
 - Key Indicator
 - Action plan
 - Recommendation
4. Connect a **Steering Date** (which corresponds to the execution frequency of interest).
5. Open the steering date properties dialog box and select the **Scheduling** tab.
6. Specify the information required for starting the campaign including:
 - the time zone to take into account (UTC, user time zone, server time zone)
 - the start date of the recurrence
 - ☛ The start date specified on the steering calendar does not correspond to the campaign start date. It simply helps 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 time
 - ☛ For details on possible configurations, see the section concerning the scheduler in the technical article "HOPEX Studio".
 - ☛ 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.

ADMINISTRATING 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

 *The key indicator category enables to specify how indicator values are interpreted, in order to compute the indicator status and Time to Failure.*
- interpretation logics


 *An indicator interpretation logic contains the logic behind the computation of the indicator status, Time to Failure, together with the list of possible statuses for the indicator.*
- indicator statuses

 *The status of an indicator enables to define whether an alert must be triggered. An indicator is computed automatically based on the latest indicator values, the aggregation period and the aggregation method.*
- Aggregation periods

 *An aggregation period is the period over which the indicator values are aggregated to compute the current key indicator value and status.*
- Aggregation methods

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


Defining Indicator Categories


 *The key indicator category enables to specify how indicator values are interpreted, in order to compute the indicator status and Time to Failure.*

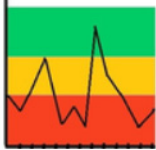
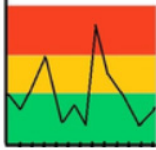
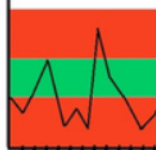
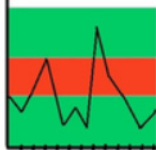
To view indicator categories:

1. 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 days before the key 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, Time to Failure, together with the list of possible statuses for the indicator.*

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 status of an indicator enables to define whether an alert must be triggered. An indicator is computed automatically based on the latest indicator values, the aggregation period and the aggregation method.

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**.

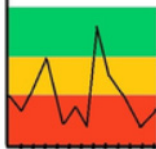
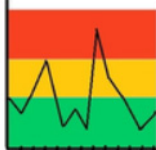
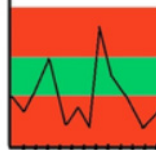

The new status you have just created will appear in the list of statuses available when creating an indicator interpretation logic. For more details, see [Defining Indicator Interpretation logics](#).

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

Aggregation periods

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

The following aggregation periods are available by default:

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

Aggregation methods

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

The following aggregation methods are available by default:

- sum
- mean
- min
- max

Creating aggregation periods or methods

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**.

Defining Key Indicator Value Computation Logics

You can define computation logics applicable to key indicator values.

Creating a computation logic

To create your own computation logic:

1. In the navigation menu, select **Administration > Indicators > Value Computation Logics**.
2. Click **New**.
3. In the properties of the created logic, specify:
 - a **Macro**
 - (Optional) **Computation Parameters**

Computation logic via query

A computation logic via query is provided by default. It counts the number of objects returned by the query.

This logic accepts two parameters:

- "Query" (mandatory)
- "ObjectParameter" (optional): if a query requires an object as a parameter, you may specify it via this parameter.

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 **Settings > 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.
 **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.

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

- ✓ Organization
- ✓ Financial Environment
- ✓ Strategic Environment
- ✓ Risk Environment
- ✓ Control Environment
- ✓ The Compliance Environment
- ✓ Responsibilities (RACI)

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

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



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 access the different organization entities:

- 1. 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 **Sub-Entities** section.*

Creating an entity

To create an entity:

1. See [Accessing organization entities](#).
2. Click **New**.

Creating a sub- entity

To create a sub-entity:

1. See [Creating an entity](#).
2. Drop it below the parent entity in the tree.

Defining entity general characteristics

In the entity property page, you can specify:

- its **Level** within the organization:
 - Business Unit
 - Sales
 - Service
- its **Status**:
 - Enabled
 - Disabled
- Its **Type**:
 - Vendor
 - Institution
 - Company
 - Public Department
 - Structure
 - Job Title
 - Generic
 - Responsible
- whether the entity is “Internal” or “External”
- its **Code**

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

Specifying responsibilities within an entity

You can specify responsible users within an entity.

Responsibilities

Risk Manager
Risk Assessor
Incident Approver

+ New
🗨️
❌
📄
✕

	Name	User Email
👤	GILL Valérie	vgill@mega.com

You can specify different roles:

- **Risk Manager**: person in charge of managing risks that have an impact on the entity.

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

direct assessments, manage assessment campaigns, define action plans, analyze and follow report creation.

- **Risk Assessor:** person in charge of completing questionnaires about risks related to the entity.
 - ☛ *You can define several risk assessors on the same entity.*
 - 📖 *The Risk assessor is responsible for assessing risks within his scope, as well as implementing action plans related to these risks.*
- **Control Assessor:** person in charge of completing questionnaires about controls related to the entity.
 - ☛ *You can define several controls assessors on the same entity.*
 - 📖 *The Control assessor is responsible for assessing and executing controls within his/her scope, as well as implementing action plans related to these controls.*
- **Incident Approver:** person in charge of approving incidents that have an impact on the entity.
- **Incident Declarant:** The incident declarant is in charge of creating incidents within his/her scope.
 - ☛ *For more details, see [Incident Management Process](#).*
 - ☛ *The incident declarant specified here will not need to specify an entity when creating an incident.*

To specify a responsibility, for example a Risk assessor:

1. In the properties page of the entity concerned, expand the **Responsibilities** section.
2. In the **Risk Assessor** tab, click **New** to define a new responsibility.
3. Select a person and click **OK**.




Scoping an entity

An entity can be connected to different object types.

A page corresponding to these object types is available in the entity properties:



- **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](#).*
- **Incidents**
- **Action plans**

A page corresponding to the following object types is available in the **Characteristics** page of the entity properties:

- **Entities**: you can specify the entity responsible for a service or management, as well as functional dependency between two entities.
- **Processes** (business and organizational processes) in which the entity takes part.
 For more details, see [Managing Processes](#).
- **Objectives** assigned to the entity.
 For more details, see [Strategic Environment](#).
- **Business Lines** for which the entity intervenes.
 For more details, see [Managing Business Lines](#).

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.

Accessing processes

To access the business / organizational process tree:

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

Root business and organizational processes are displayed.

Process hierarchy

The hierarchy of processes/operations is as follows:



For each process of the hierarchy the following is displayed:

- Risks (directly connected to processes)
 - Controls (directly connected to risks, which are in turn connected to processes)
- Controls (directly connected to processes)

The following columns are available:

- **Risks** (number of)
- **Controls** (number of)
- **Last assessment**
- **Residual risk**



The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

- **Forecast risk**



Forecast risk represents the residual risk forecast for the year to come.

- **Latest compliance rate**



The compliance rate is the percentage of "Pass" controls.

- **Control level**



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

Specifying process characteristics

To access the characteristics of a process:




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

The **Owner** is responsible for global operation of the process in terms of effectiveness, profitability and security.

Specifying process scope

A process can be linked to different objects types.






A specific page is available in the process properties for each object type:

- **Risks:** risks that relate to the process.
 For more details, see [Managing Risks](#).
- **Controls:** controls that relate to the process.
 For more details, see [Managing Controls](#).
- **Incidents**
- **Action plans**
 To view regulations impacting a process, expand the **Regulatory Impact** section.

Specifying process responsibilities

Responsibilities on a process are shared by persons with different roles.

To specify responsibilities on a process:

- 1 In the process properties, expand the **Responsibilities** section.
You can specify the following responsibilities:
 - **Accountable**
 - **Consulted**
 - **Informed**
 The above responsibilities correspond to the RACI responsibilities. See [Responsibilities \(RACI\)](#).
 - **Risk assessor**
 The Risk assessor is responsible for assessing risks within his scope, as well as implementing action plans related to these risks.
 You can define several risk assessors on the same entity.
 - **Control assessor**
 The Control assessor is responsible for assessing and executing controls within his/her scope, as well as implementing action plans related to these controls.
 You can define several Control assessors on the same entity.

Specifying sub-processes

To specify the sub-processes of a business process:

- 1 In the business process properties, expand the **Sub-processes** section.
You can specify:
 - The business process components
 - The connected organizational processes

To specify the sub-processes of an organizational process:

- 1 In organizational process properties, expand the **Sub-processes and Operations** section.
You can specify:
 - organizational processes
 - associated operations

Managing business continuity

☛ These features are available with **HOPEX BCM** only.

To access the Business Impact Analyses (BIAs) and Business Continuity Plans (BCPs) associated to a business process:

- 1 Open business process properties and select the **Business Continuity** page.

☛ For more details, see:

- [Defining a Business Impact Analysis](#)
- [Designing a Business Continuity Plan](#)

To add a business process to a BCM system:

- 1 In a business process pop-up menu, select **Add to BCM system**.

☛ For more details, see [Managing BCM Systems](#).

To create a Business Impact Analysis (BIA) from a business/organizational process:

- 1 Open the process pop-up menu and select **Create a BIA**.

Other sections of a process

The properties page of a process presents the following sections:

- **Objectives:** see [Strategic Environment](#)
- **IT assets:** IT resources (applications, databases and servers) are made available for process implementation.
 - ☛ See [Managing Applications](#).
- **Entities** that intervene in the process.
 - ☛ See [Managing Entities](#).
- **Business Lines:** business lines that use the process services.
 - ☛ See [Managing Business Lines](#).

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.

Accessing Business Lines

To access the different organization business lines:

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

From this page you can view trees of organization business lines, 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:

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

Connecting entities and processes to a business line

A business line can be implemented by an entity within the framework of a process.

To connect a business line to entities and processes:

- 】 In the business line properties, expand the following sections:

- **Entities**

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

- **Processes**

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

Defining risks and incidents that impact a business line

To specify risks that impact a business line:

- 】 In the business line properties, select the pages:

- **Risks**

- **Incidents**

Entering gross revenues for incident management


The **HOPEX IRM** desktop enables the Incident and Loss Manager to enter gross incomes for the organization so as to perform a BIA analysis (Basel II Basic Indicator Approach).

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

To specify gross revenues that impact a business line:

1. In the properties of a business line select the **Gross revenues** page.
2. Connect or create a gross income.

Managing Applications

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

Accessing applications

To access applications:

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

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 processes supported or business lines:

- 】 Open the properties of the application and select:
 - **Characteristics > Business / Organizational processes**, or
 - **Characteristics > Business Lines**.

You can connect other object types in specific pages of application properties:

- **Risks**
- **Controls**
- **Action plans**
- **Incidents**
- **Deficiencies**


FINANCIAL ENVIRONMENT

To access components of the financial environment:

1. In the navigation menu, click **Environment > Financial**.


Accounts

This tree displays controls associated to each account.

 These accounts are to be monitored withing the framework of SOX compliance.

Characteristics of an account

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
- **Sub-accounts:** the account may consist of sub-accounts.
- **Entities** and **Processes:** you may connect the account to entities and processes.
- **Incident Financial Elements:**
 - Loss
 - Gain
 - Recovery
 - Provision

Connecting controls to an account

To connect controls to an account:

1. In the account properties, select the **Controls** page.
2. Connect one or more controls.

Products

This tree displays open issues related to the product.



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.

To create or connect incidents to a product:

1. Open the product properties and select the **Incidents** page.
2. Create or connect incidents.

You can view, for each incident:

- its status
- its declaration date
- the declarant's entity
- associated losses

Gross Incomes

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

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

To create a gross income:

1. Click **Environment > Financial > Gross Incomes**.
2. Click **New**.
3. Enter the following properties:
 - **Business line**
 - **Begin Date** and **End Date**
 - **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:

- 1 In the navigation menu, select **Environment > Objectives**.

To create an objective:

- 1 Click the **New** button.

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:

- 1 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:

1. 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.

- **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.

Creating a risk type

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.

Analyzing the impacts of a risk type

A report enables you to view the impacts of a risk type. See [Risk Type Analysis Breakdown Report](#).

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:

- 1 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 and access sub-control types:

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



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:

- 】 Click the + sign of the control type of interest.
For each control type, the number of first level controls is displayed.

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

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

THE COMPLIANCE ENVIRONMENT

 The features available in the **Environment** menu are available to manager profiles only (IRM managers and Control director).

HOPEX IRM enables you to manage the regulatory environment of your organization as well as its business policies.

To manage your compliance environment in **HOPEX**:

- 1 In the navigation menu, select **Environment > Compliance**.

You can:

- import UCF content from a Shared List of the Common Controls Hub and define articles that apply to your organization.
- manually create regulatory frameworks, articles and control directives



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), or standards.



An article is a citation from a regulatory framework and is usually associated to a mandated control directive.



Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

- create manually policy frameworks and business policies.



A policy framework consists of a set of business policies. Policy frameworks may contain sections.

Managing your Regulatory Environment

Using UCF Import

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 relevant data from the UCF Common Controls Hub (Authority Documents, Citations and Controls)
- declaring the appropriate articles as relevant for your organization: see [Defining Applicable Regulations and Business Policies](#).

To import UCF data:

1. In the navigation menu, select **Environment > Compliance > Regulatory Frameworks**.
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?	<div>Last Imported UCF Update</div> <div>Latest Available UCF Update</div>
<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**.

☛ Once UCF data has been imported into **HOPEX**, it is not possible to export it to transfer it to another repository.

Creating Regulatory Content Manually

Creating regulatory frameworks and their content

If you do not use UCF import, you can create your own regulatory content.

☛ The regulatory content you manually create is automatically considered as applicable.

To create a regulatory framework:

1. In the navigation menu, click **Environment > Compliance > Regulatory frameworks**.
2. Click **New**.

📖 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), or standards.

To create content for your regulatory framework:

1. In the navigation menu, click **Environment > Compliance > Regulatory frameworks**.
2. Right-click the regulatory framework and select:
 - **New > Section**

📖 A section is a citation from a regulatory framework without any mandated control directive, but containing other sections or articles.

- **New > Article**

📖 An article is a citation from a regulatory framework and is usually associated to a mandated control directive.

Creating control directives

To create control directives:

1. In the navigation menu, click **Environment > Compliance > Control Framework**.

2. Right-click the root of the tree and select **New > Control Directive**.



Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

Managing Business Policies

HOPEX IRM enables you to manage both business policies and regulations.

Creating business policies

You can create policy frameworks and their content (business policies).



A policy framework consists of a set of business policies. Policy frameworks may contain sections.

To create a policy framework:

1. In the navigation menu, select **Environment > Compliance > Policy Frameworks**.
2. Click **New**.

To create policy framework content:

3. Right-click the policy framework you have just created and select:
 - **New > Policy Framework Section**
 - **New > Business Policy**

Defining Applicable Regulations and Business Policies

Regulatory content applicability

If you imported UCF content, you need to define the content applicable to your organization. All the articles/sections of a regulatory framework are not applicable to your organization.



The regulatory content you created manually automatically applies to your organization.

Compliance officers can inspect the imported regulatory frameworks and specify which ones are applicable. Only applicable content can be viewed by stakeholders in **HOPEX** registers. See [Managing the Compliance Register](#).

Reviewing regulatory frameworks after UCF import

Once the UCF data has been imported, a tree appears in the **Environment** menu available to manager profiles.

This tree displays:


- regulatory frameworks (Authority Documents)
- citations (Citations)
- associated control directives (Common 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 the regulatory content applicable to your organization

 *The regulatory content you created previously is automatically considered as applicable.*

To declare regulatory content as applicable:

1. from the navigation menu, select **Environment > Compliance > Regulatory Frameworks**.
2. Expand the tree if necessary and select the check-box corresponding to the regulatory frameworks/articles/sections you must comply with.

 *The grey square  means that the regulatory content below has been partially selected only.*

Defining the Scope of Regulations and Business Policies


You can define the scope of your regulatory frameworks and policy frameworks, that is to say subjected elements.

To do this:

1. In the navigation menu, select:
 - **Environment > Compliance > Regulatory Frameworks**, or
 - **Environment > Compliance > Policy Frameworks**.
2. In the properties of a regulatory or business policy element, expand the **Subjected Elements** section.
3. Connect entities, applications, or processes.

RESPONSIBILITIES (RACI)

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	Explanation
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:

1. In an object property pages, expand the **Responsibilities** section.
2. Create responsibility assignations in one of the following tabs:
 - **Responsible**
 - **Accountable**
 - **Consulted**
 - **Informed.**

MANAGING KEY INDICATORS



A key indicator is a metric used by organizations to provide an early warning of increasing risk exposures in various areas of the enterprise.

Indicators 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**.*

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

ACCESSING KEY INDICATORS

To access key indicators from a list:

- 1 In the IRM desktop, select **Registers > Indicators** .
A list of all the indicators of your environment is displayed.

The following information is displayed in columns for each indicator:

- Current Status
- Last Measurement (days)
- Time to Failure (days)



Time to failure is the number of days before the key indicator turns to "Failed" status.

- Value
- Lower Threshold
- Higher Threshold
- Entities



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

DEFINING KEY INDICATORS

Creating a Key Indicator

To create a key indicator:

1. In the IRM desktop, select **Registers > Indicators**.
2. Click **New**.
A creation window opens.
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 the values within the thresholds are accepted.
 - **Rejected Values**: all values within the defined thresholds are rejected.

☛ For more details, 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 details, 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 key indicator category, aggregation period and aggregation method after the key indicator 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, clear 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 key 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 key indicator aggregated values in order to compute the indicator current value and status.

- Sum
- Average
- Min
- Max

☛ *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



A key indicator is a metric 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.

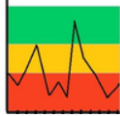
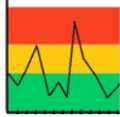
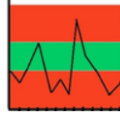
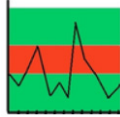
In this example the different characteristics described in **HOPEX** are as follows:

- **Lower Threshold** 900k
- **Higher Threshold** 1,1 million
- **Category**: Standard (all values beyond the upper limit are considered satisfactory)
- **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

 The key indicator category enables to specify how indicator values are interpreted, in order to compute the indicator status and Time to Failure.

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.	

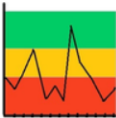
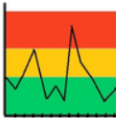
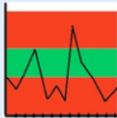
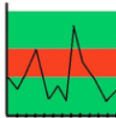
Relation between Indicator Category and Interpretation Logic

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:

Category

Standard
Reverse
Accepted Values
Rejected Values

Key Indicator Interpretation Logic*

My Interpretation logic for Accepted Values


Accepted Values (HOPEX)

My Interpretation logic for Accepted Values

➡ 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 key indicator category, aggregation period and aggregation method after the key indicator 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. See [Accessing Key Indicators](#).
2. In the **Characteristics** indicator property page, expand the **Advanced** section.
3. Click **Edit Parameters**.

In the window that opens, you can edit:

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



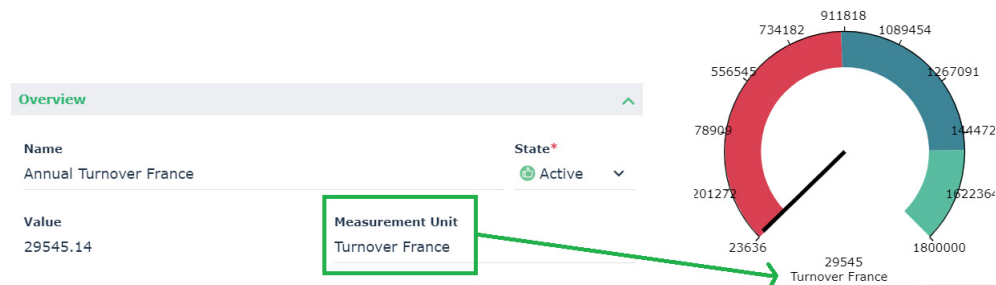
Time to failure is the number of days before the key indicator turns to "Failed" status.

 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 details 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. See [Accessing Key Indicators](#).
2. Open the key indicator property page.
3. 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:

1. See [Accessing Key Indicators](#).
2. In the property page of the indicator, select the **Characteristics** page and expand the **Scope** section.

Here you can specify the associated objects:

- 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 process



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 indicators to 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. See [Accessing Key Indicators](#).
2. In the properties of a key indicator, select the **Action Plans** page.
3. 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.

Connecting Risks

To connect risks to a key indicator:

1. See [Accessing Key Indicators](#).
2. In the property page of the key indicator, select the **Characteristics** page and expand the **Risks** section.
3. Connect an existing risk or create one.

CONSULTING THE KEY INDICATOR DASHBOARD

To consult your key indicator dashboard:

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

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

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 details, 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 key indicator value and status.*

- the aggregation method

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

☛ *For more details, see [Specifying the Aggregation Period and Method](#).*

The key indicator status is computed when:


- a new value is added
 For more details, 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 details, see [Activating / Deactivating a Key Indicator](#).

Time to Failure

Time to failure is the number of days before the key 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 details, 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.  9999 is displayed in the Time to Failure column of the list of indicators.
0 day(s)	The indicator status is "Failed" already.

Last Measurement of the Key Indicator


Last Measurement indicates the number of days elapsed since an indicator value was last entered.

This value is rounded to the closest integer.

Key Indicator Value

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

The indicator value is the last aggregated measurement of the key indicator.

 If no aggregation period or method have been defined, it is 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 a key 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 Notifications

HOPEX IRM enables to send automatic notifications based on:

- the key indicator status
- the last measurement date
- The Time to Failure value (number of days)

This way, you can ensure that the indicator owners properly manage indicators.

To specify or modify user notifications:

1. See [Accessing Key Indicators](#).
2. In the properties 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 details, 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 key indicator values in order to feed the key indicator.

It is also possible to feed automatically the key indicator.

Entering a key indicator value manually

To enter a key indicator value:

1. See [Accessing Key Indicators](#).
2. In the properties of a key indicator, select the **Values** page.
3. Expand the **Values** section and click **New** to enter a value.
4. Modify the default date if necessary.
5. 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 Notifications](#).

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

Parameterizing automatic value entering

It is also possible to feed automatically the key indicator.

To do this:

1. See [Accessing Key Indicators](#).
2. In the properties of a key indicator, select the **Values** page.
3. In the **Measurement Parameters** section, select the **Measurement Frequency** through a steering calendar.
4. Select the **Indicator Value Computation Logic**.

 For more details, see [Defining Key Indicator Value Computation Logics](#).

5. (optional) If the selected computation logic requires parameters, specify the query in the **Computation Parameters** field.

Query =

ObjectParameter =

A button enables you to **Test the calculation**.

VIEWING THE INDICATOR GRAPH

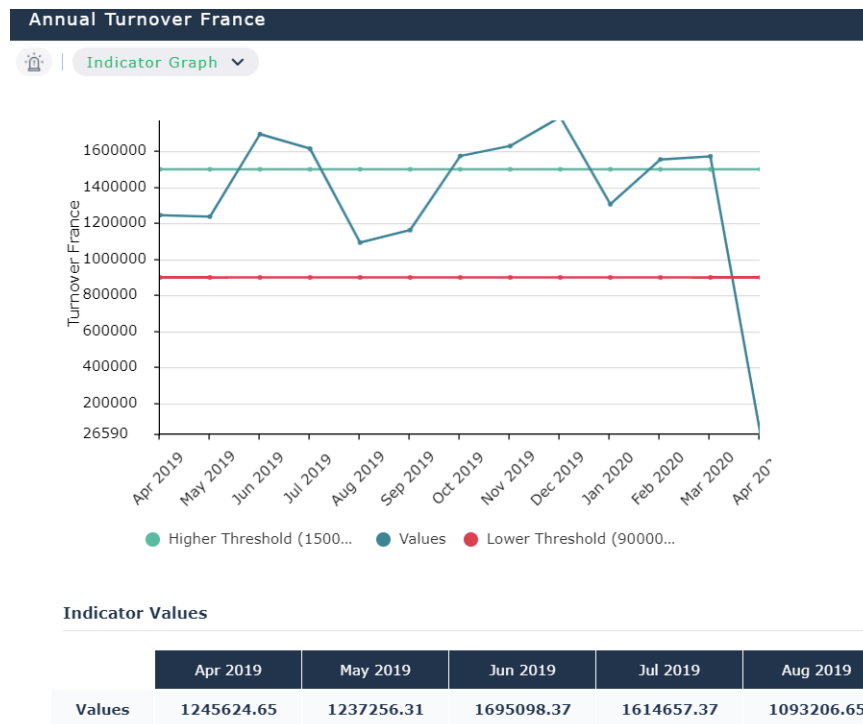
HOPEX IRM enables you to display an indicator graph for a specific indicator.

To access this graph:

1. See [Accessing Key Indicators](#).
2. 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 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.

- ✓ [Accessing Assessments by Profiles](#)
- ✓ [Accessing Assessment Templates](#)
- ✓ [Preparing the Assessment Environment](#)
- ✓ [Starting an Assessment Campaign](#)
- ✓ [Completing Questionnaires](#)
- ✓ [Following up assessments progress](#)

➡ You can also directly assess risks and controls, without using questionnaires. See "Direct Assessment" in **HOPEX Enterprise Risk Management** and **HOPEX Internal Control** documentation.

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	<ul style="list-style-type: none">- Accept or refuse questionnairesReply to questionnaires	IRM Contributor desktop

ACCESSING ASSESSMENT TEMPLATES

To access assessment templates:

- 1 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.

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.

For more details on assessment template customization, see [Managing Assessment Templates](#).

PREPARING THE ASSESSMENT ENVIRONMENT

Before starting an assessment campaign, you must first fill in prerequisites.

Prerequisites to Risk Assessment

For risk assessment, see [Prerequisites to Risk Assessment](#).

Pre-requisites to Control Assessment

For control assessment, see the prerequisites in the sections corresponding to the different assessment templates.

- [Control Assessment by Entity](#)
- [Control Assessment by Entity and Regulatory Framework](#)

STARTING AN ASSESSMENT CAMPAIGN

Creating Assessment Campaigns

To create an assessment campaign in **HOPEX IRM**:

1. In the navigation menu, click **Assessment > Campaigns**.
2. Click **New**.
3. To define the object type to which the campaign relates:
 - Risk (**Risk assessment**)
 - Control (**Control assessment**)
4. Click **Next**.
The campaign creation page appears.
5. Specify the campaign **Name**.
6. (optional) Select the assessment **Template**.
 - ☞ Depending on the type of object selected, several assessment templates are offered.
 - ☞ You can choose not to use an assessment template. Doing so, you can define the scope of each of your assessment session. See [Creating an Assessment Session Manually](#).
7. Modify the **Calendar** if required.
 - ☞ The calendar serves to initialize the begin and end dates of the evaluation campaign.
8. Specify the **Begin Date** and the **End Date**.
9. Click **Next**.

10. In the **Scope Selection** window, select the objects that define the evaluation 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.

☛ *Some columns give indications to help you decide which risks or controls need to be assessed.*

	Assessment Freshness	Net Risk	Open Incidents	Forecast Risk
<input type="checkbox"/> MyCompany				
<input checked="" type="checkbox"/> World@Hand Corporation				
<input type="checkbox"/> Corporate Headquarter				
<input checked="" type="checkbox"/> Regional Headquarter				
<input type="checkbox"/> Car Rental Department				
<input checked="" type="checkbox"/> HR Department				
<input checked="" type="checkbox"/> Architecture lacks flexibility	None	None	0	None
<input checked="" type="checkbox"/> Forged invoice (purchase)	None	None	0	None
<input checked="" type="checkbox"/> Goods receipt inconsistent w...	None	None	0	None

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

☛ *If you deselect a node of a branch, only the child elements of this branch are deselected.*

11. Click **Next**.
12. Look at the campaign summary.
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**
 - possible **errors** (it is not possible to launch the campaign without specifying some specific information, for example respondents)
 - **Warnings**, for information purpose (for example: missing e-mails)
13. Click **Next**.

14. In the page dedicated to planning, specify when you want the campaign to be started:
 - **Immediately**

☛ If you choose this option, the campaign is started as soon as you click **OK**.
 - **Specific Time and Date**

☛ Your questionnaires will be sent to respondents at a specified date and time. This is the recommended option.
 - **Not now**

☛ No questionnaires are sent. You will need to manually create an assessment session when you are ready to plan the sending of questionnaires.

☛ See [Creating an Assessment Session Manually](#).
15. Click **OK**.

Creating an Assessment Session Manually


You need to create one or several assessment session(s) manually:

- if you chose not to base your assessment campaign on an assessment template.
- If you selected the scheduling option “Not now” when creating an assessment campaign.

☛ See Previous step: [Creating Assessment Campaigns](#).

To create an assessment session:

1. In the properties page of the assessment campaign, select the **Sessions** page.
2. Click **New** then **Next**.
3. Select the session scope, that is to say the objects to be assessed in their context.

Creation of Assessment Session - Select Scope				
	Select all objects you want to include in this Assessment Session. For objects which are not valid, make sure to provide a Respo			
<input type="checkbox"/>	Status	Assessed Object	Context	Respondent
<input type="checkbox"/>	✓ Valid	⚠ Financial Loss	Account Management	👤 Alex
<input type="checkbox"/>	✓ Valid	⚠ Financial Loss	Account Management	👤 Adam

☛ Only valid objects (for which a respondent and an e-mail have been specified) can be selected.

In the example below, “Financial Loss” can be assessed in the “Account Management” context by two respondents. You can therefore select two “assessment nodes” (object+context+respondent).

4. Click **Next**.
5. In the planning page, select whether you want to send questionnaires:
 - **Immediately**
 - at a **Specific Time and Date**If you select "Immediately", an assessment session is started right now.

COMPLETING QUESTIONNAIRES

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

See [Managing Questionnaires](#) in the documentation about HOPEX general features.

FOLLOWING UP ASSESSMENTS PROGRESS

Consulting Session Results

To consult progress of an assessment session:

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

Viewing assessment campaign results

To view the results (answers) of an assessment campaign:

1. Open the properties of an assessment campaign and select the **Results** page.

In this page, all the campaign assessment nodes are listed. The following information is given for each of them:

- Assessed object
- Assessment context
- Respondent
- Answer Date
- Each question label

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.

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.

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](#)

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

- [Risk-Related Reports](#)
- [Reports Related to Controls](#)
- [IT Regulatory Compliance Reports](#)
- [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	Compliance	Incident	Action plans
GRC manager	X	X	X	X	X
Risk Manager	X				X
Internal Control Director		X	X		X
Risk Manager Incident and Loss Administrator	X		X	X	X

See also:

- [Action Plan Follow-up Reports](#)
- [IT Regulatory Compliance Reports](#)

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 key indicators:

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

The following reports are available:

- Indicator comparator
- Multi-Gauge chart
- Multi-line chart

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

Indicator Comparator

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

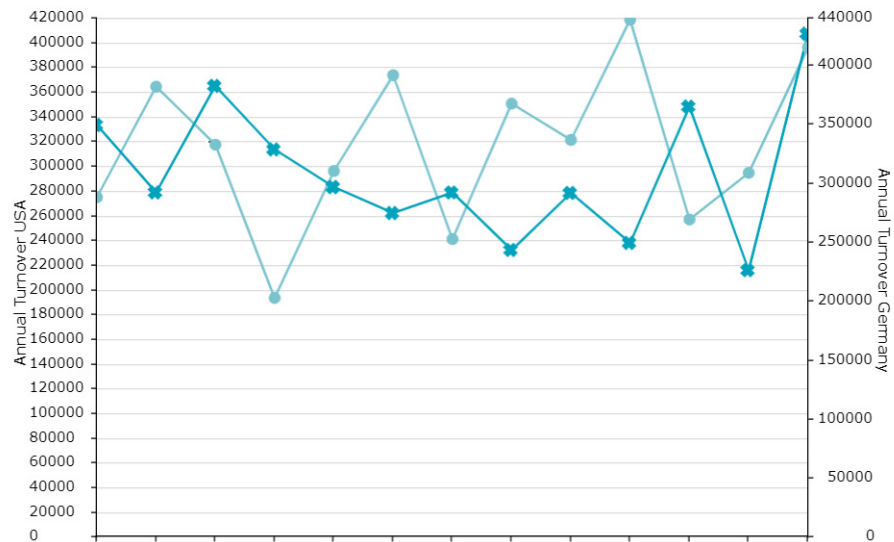
Access path

Analysis > Indicators > Indicator comparator

Parameters

Parameters	Remarks
Primary Key Indicator	Mandatory
Secondary Key Indicator	Mandatory
Aggregation Period	Mandatory
Aggregation method	Mandatory
Value start date	Optional
Value end date	Optional

Results



Multi-Gauge chart

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

Access path

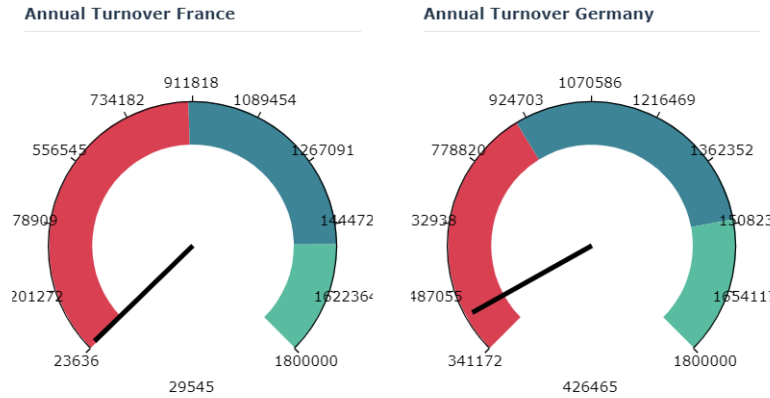
Analysis > Indicators > Multi-gauge charts

Parameters

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

Results

France vs Germany



Multi-line chart

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

Access path

Analysis > Indicators > Multi-line chart

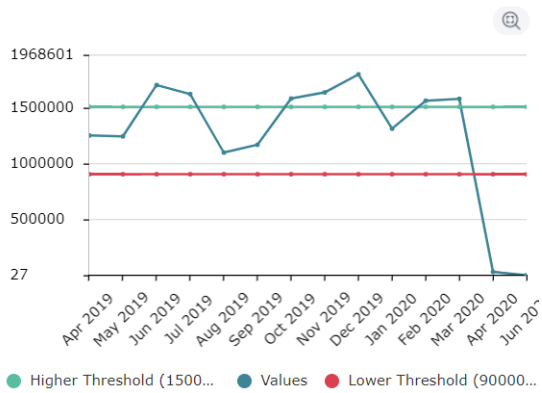
Parameters

Parameters	Remarks
Number of columns	Mandatory
Key Indicators	Mandatory
Value start date	Optional
Value end date	Optional

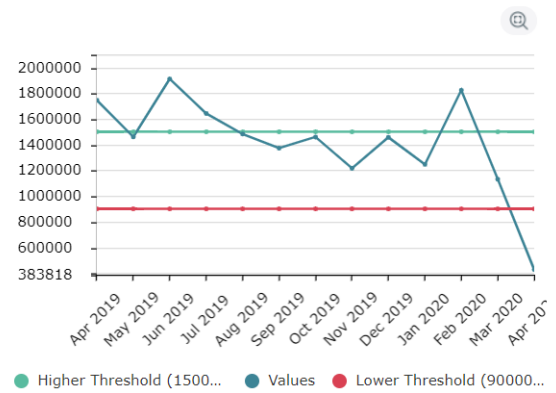
Results

France vs. Germany

Annual Turnover France



Annual Turnover Germany



ACTION PLAN FOLLOW-UP REPORTS

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

See also: [IRM Report Availability](#)

Action Plan Follow-Up

To follow up action plans:

- 1 Select **Analysis > Remediation > Follow-Up**.

Access path

Analysis > Remediation > 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
- Mean
- 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

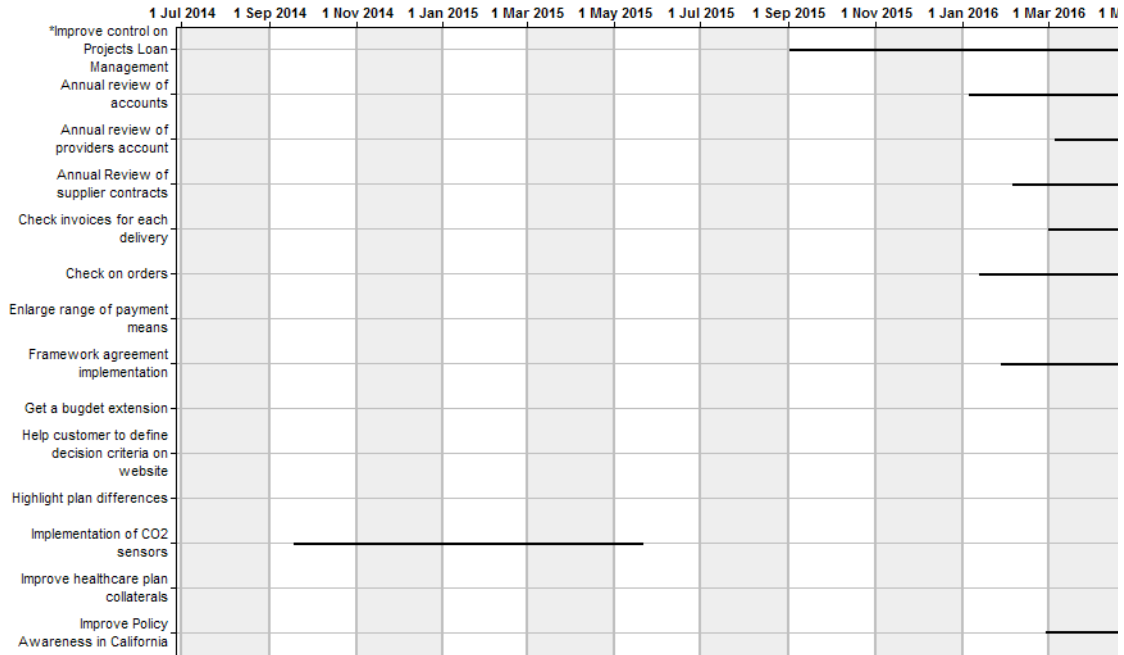
This report displays all action plans in the form of a Gantt chart.

To generate a Gantt chart of action plans:

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

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

1. Action Plan Gantt





IRM SOLUTION WORKFLOWS

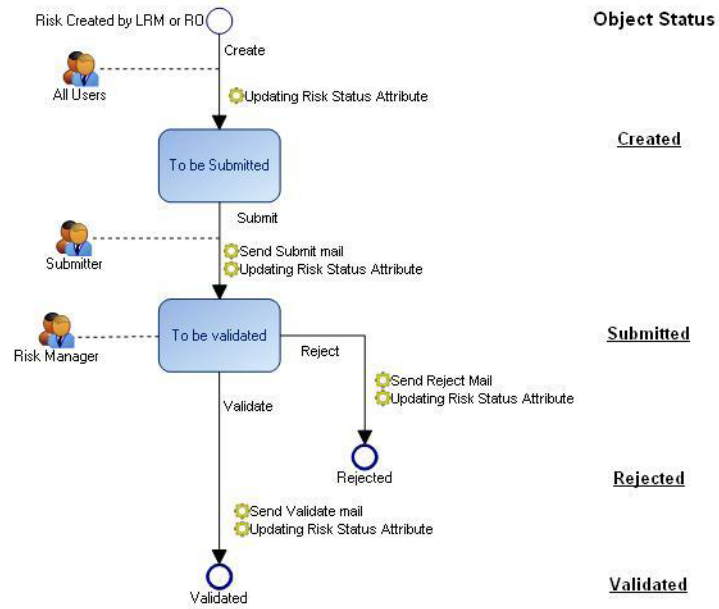


IRM (Integration Risk Management) activities are performed via ready-to-use workflows.

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

- ✓ [Risk Workflows](#)
- ✓ [Testing Workflows](#)
- ✓ [Action Plan Workflows](#)
- ✓ [Incident Workflow](#)
- ✓ [Campaign Workflow](#)

RISK WORKFLOWS

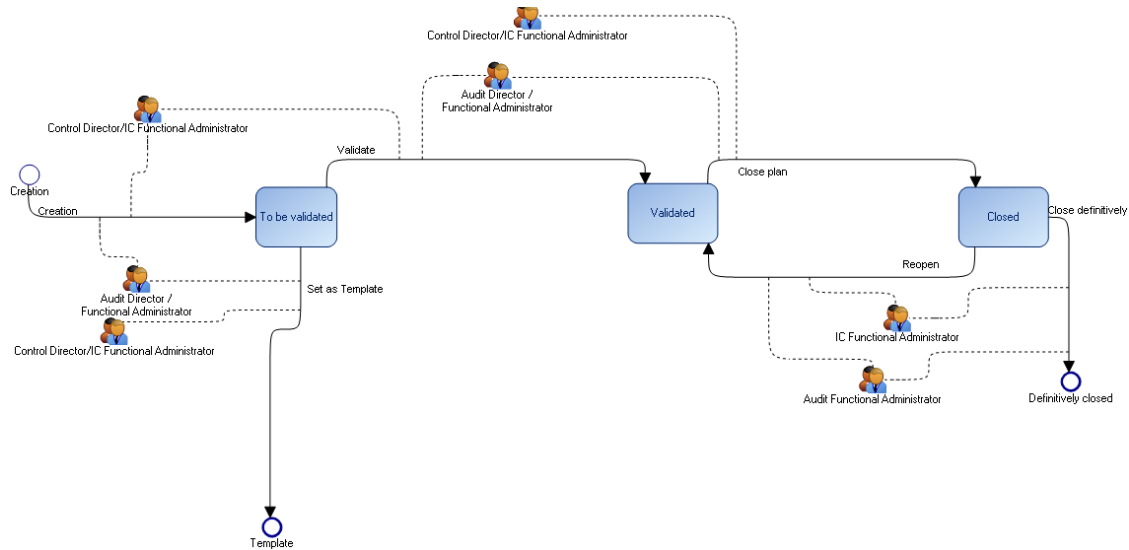


➡ For more details on the characteristics of risks and risk-related workflow, see [Managing Risks](#).

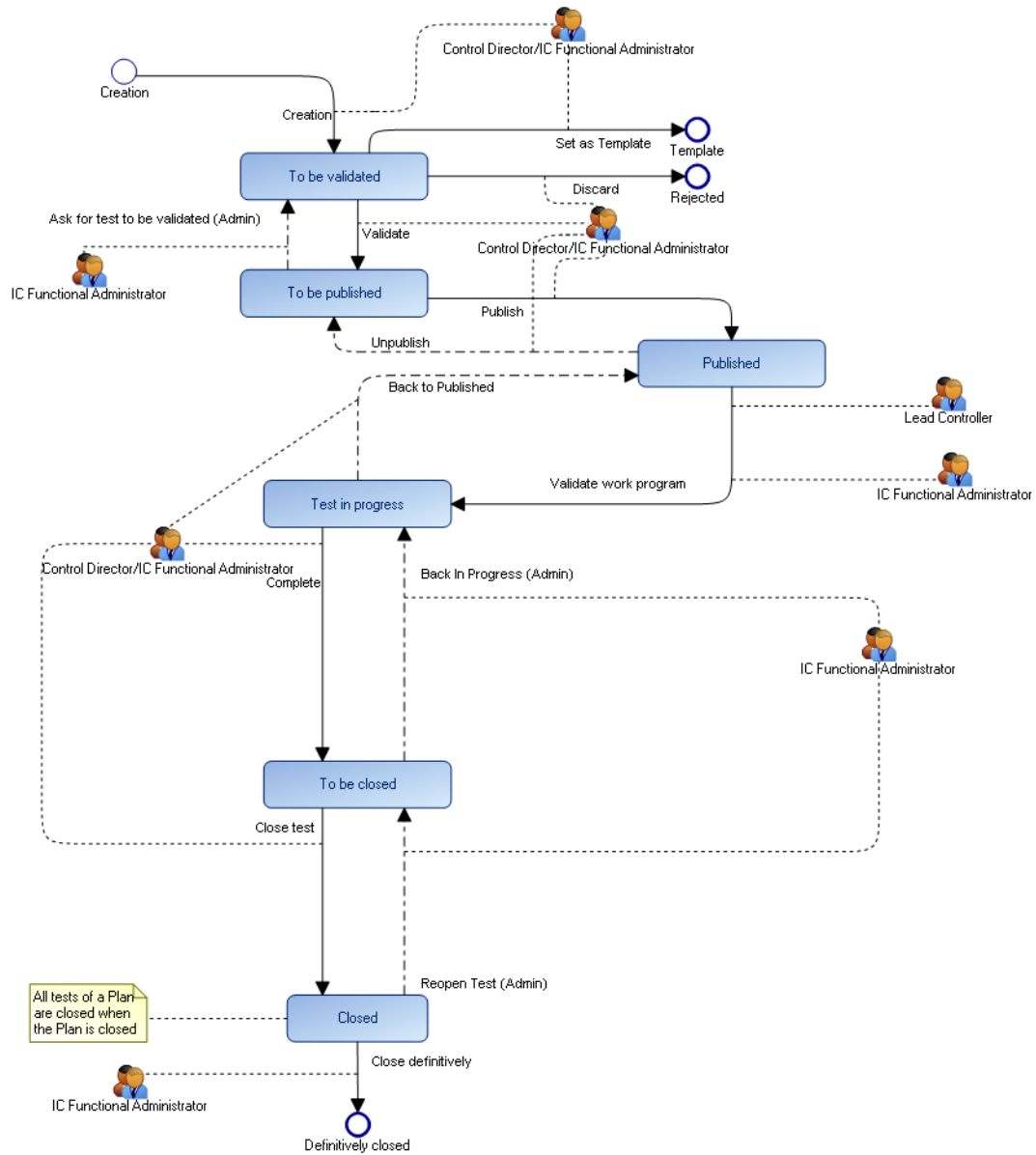
TESTING WORKFLOWS

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

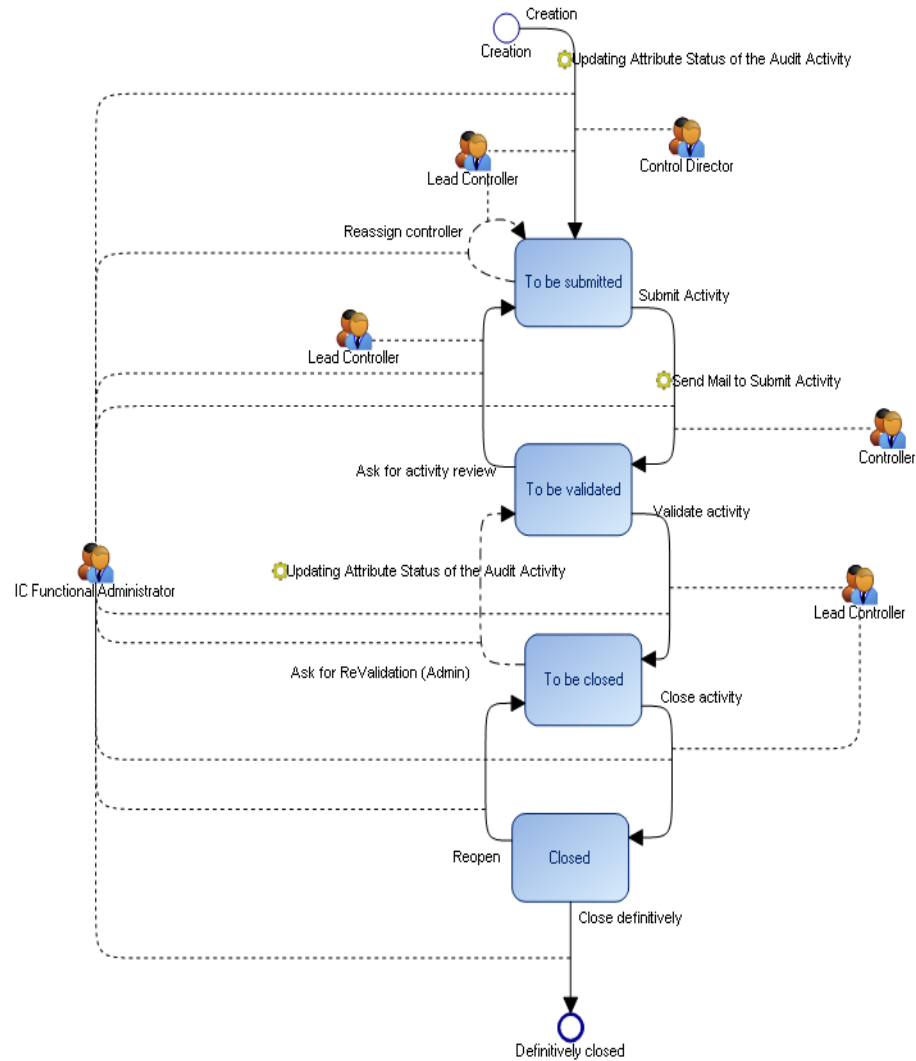
Test Plan/Audit Plan Workflow



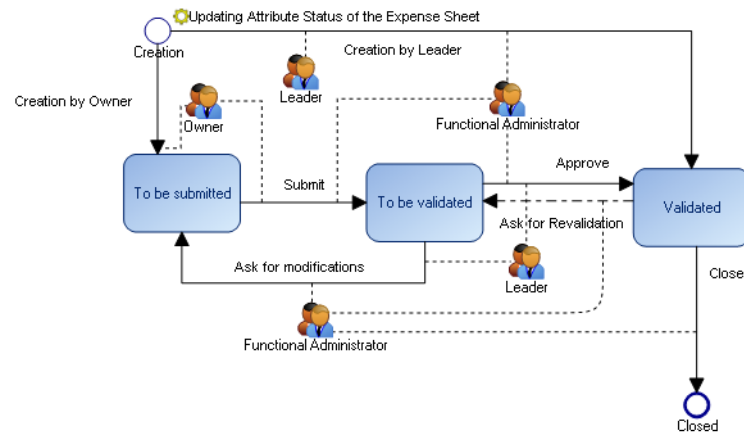
Test Workflow



Test Activity Workflow



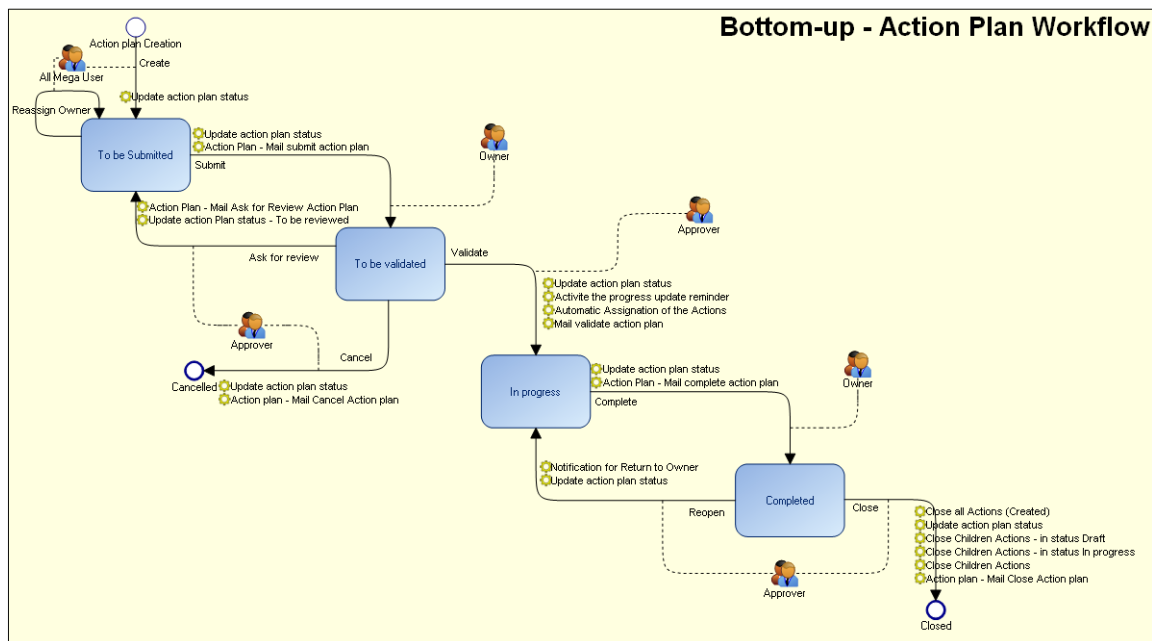
Expense Sheet Workflow



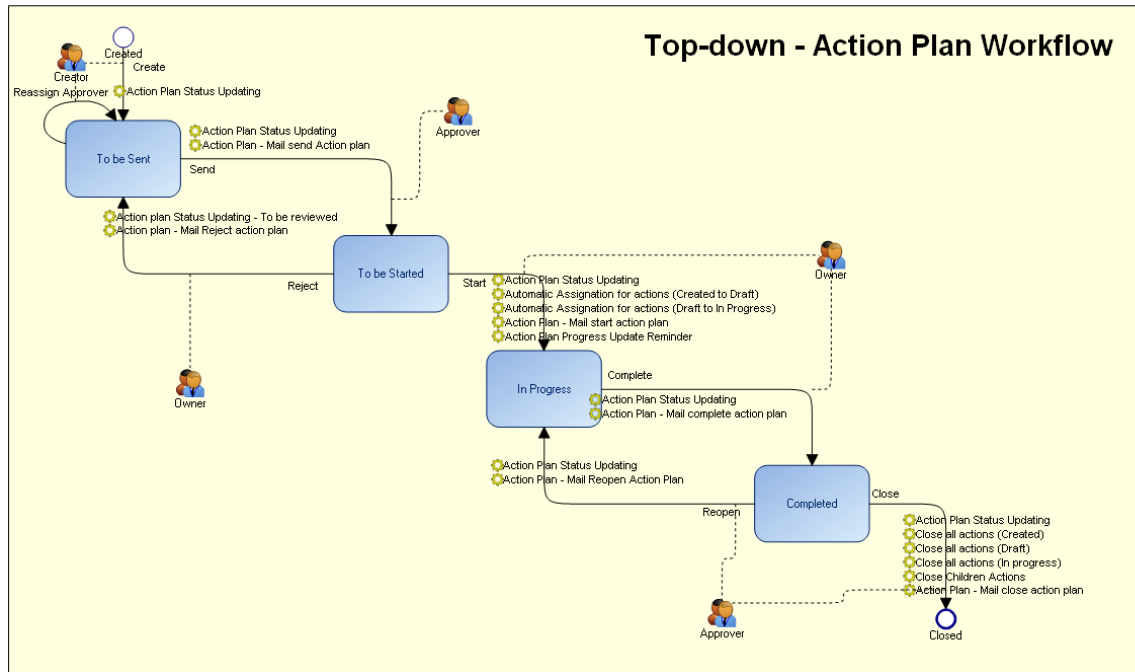
ACTION PLAN WORKFLOWS

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

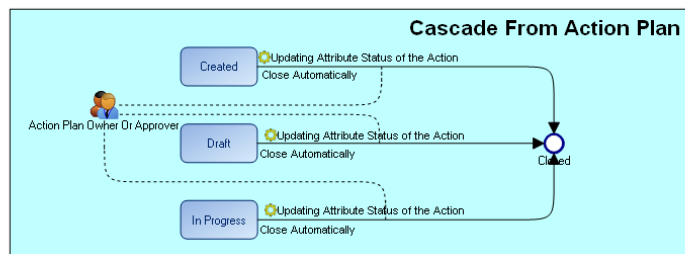
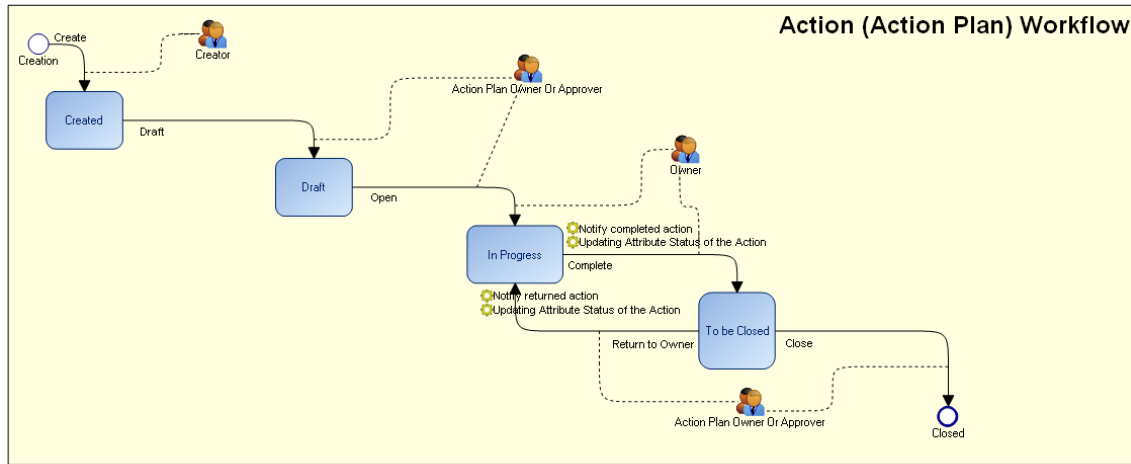
"Bottom-up" Action Plan Workflow



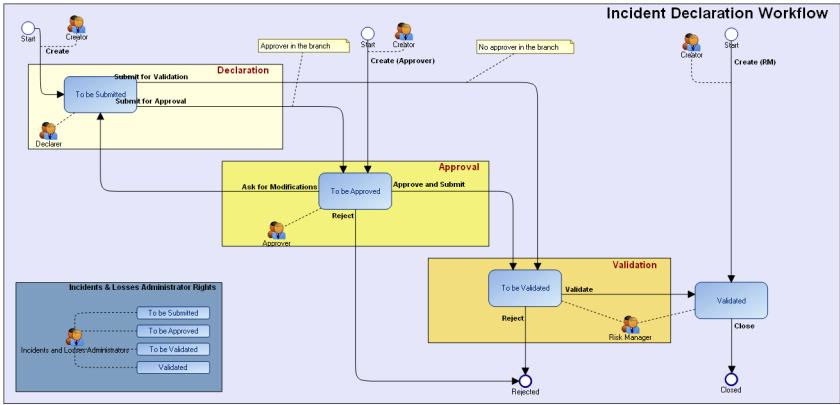
"Top-down" Action Plan Workflow



Action Workflow



INCIDENT WORKFLOW



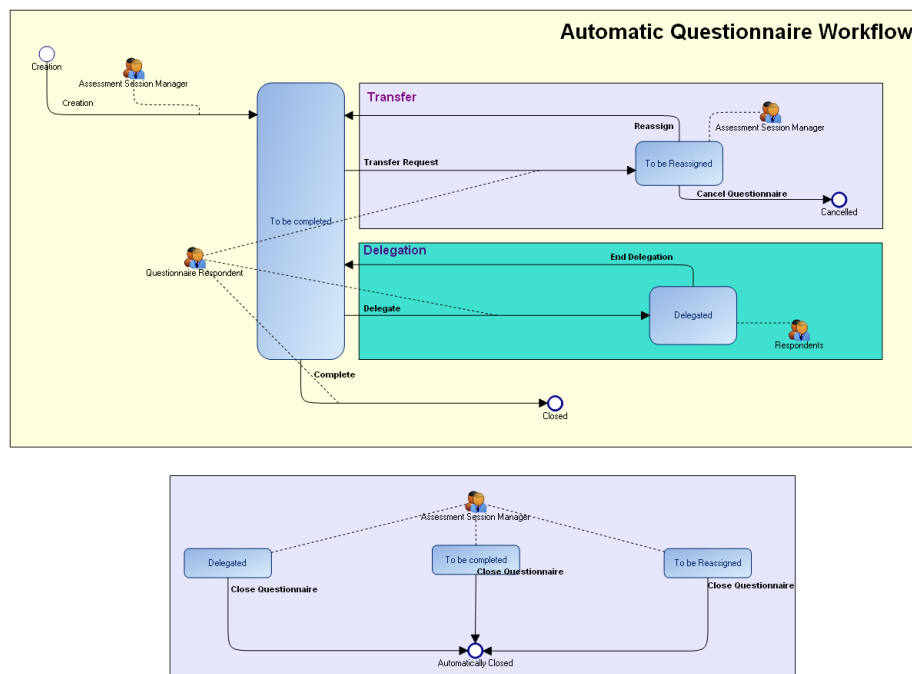
➡ For more details on incidents, see [Incident Management Process](#).

CAMPAIGN WORKFLOW

Assessment Campaign Workflow

See [Assessment Workflows](#).

Execution (Automatic) Campaign Workflow





THE IRM CONTRIBUTOR DESKTOP



A specific desktop enables you to contribute to IRM (Integrated Risk Management) concerns.

This desktop is available to business users of the following solutions:

- **HOPEX Enterprise Risk Management (ERM)**
- **HOPEX Internal Audit (Audit)**
- **HOPEX Internal Control (CI)**
- **HOPEX LDC LDC**
- **HOPEX BCM**

☛ *You can access the features and menus of the solution(s) used.*

- ✓ [Presentation of the IRM Contributor Desktop](#)
- ✓ [Viewing your Environment](#)
- ✓ [Dashboard and Widgets](#)
- ✓ [Managing Incidents](#)
- ✓ [Managing Action Plans and Actions](#)
- ✓ [Managing Recommendations](#)
- ✓ [Managing Questionnaires and Check-lists](#)
- ✓ [Creating Risks and Controls](#)
- ✓ [Managing Key Indicators](#)
- ✓ [Performing a BIA \(Business Impact Analysis\)](#)
- ✓ [Taking Part in Business Continuity Plans](#)

PRESENTATION OF THE IRM CONTRIBUTOR DESKTOP

Accessing the IRM Contributor Desktop

To access the IRM Contributor Desktop:

1. See [Connecting to HOPEX](#).
2. Login with the "IRM Contributor" profile.

Features Available to the IRM Contributor

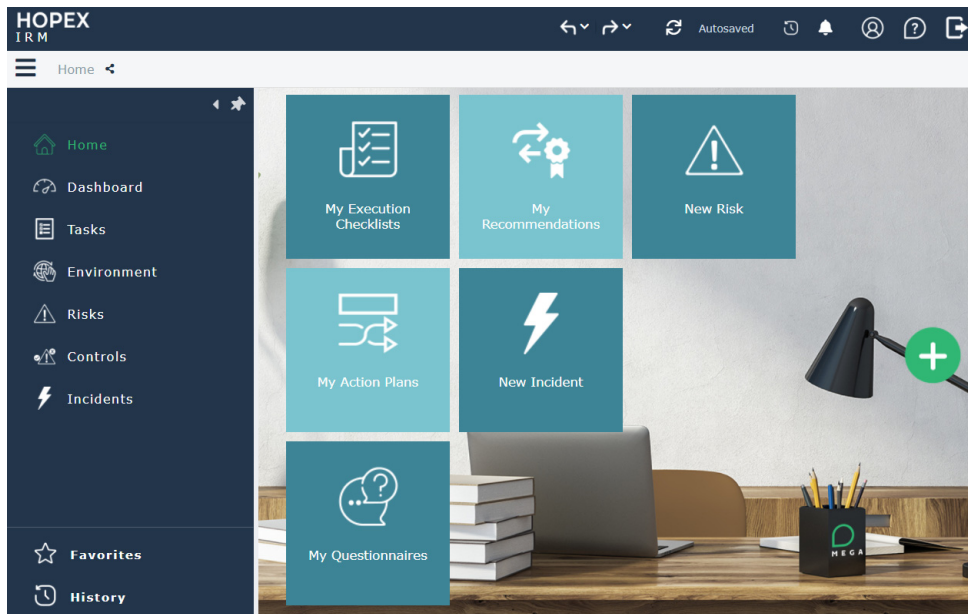
Find below the object types and features available depending on the solution used.

Features/Solutions	ERM	IC	LDC	Audit	BCM
Generalities - Viewing the environment (Viewing your Environment) - Viewing and exporting dashboard reports	X	X	X	X	
Risks - Identifying risks - Answering assessment questionnaires (See: Answering a Questionnaire)	X				
Controls - Creating Controls - Answering assessment questionnaires (See: Answering a Questionnaire)	X	X			
Control Execution - Completing Execution Check-Lists (See Completing Assessment Check-lists).		X			
Action Plans /Actions - Viewing and following-up action plans - Creating actions (See Managing Action Plans and Actions).	X	X	X	X	
Recommendations - Viewing recommendations (See Managing Recommendations).				X	
Incidents - Declaring incidents (See Managing Incidents).			X		
Key Indicators - Enter a key indicator value (See Enter a key indicator value).	X	X			
Business Impact Analysis - Fill in a BIA matrix (See Performing a BIA (Business Impact Analysis)).					X
Take part in Business Continuity Plans (BCPs): - tested by ongoing exercises - triggered within the framework of crises (see Taking Part in Business Continuity Plans)					X

Home Page

The home page provides tiles that you can use to perform the most common tasks on the objects that you work with.

☛ *The tiles and menus displayed depend on the solution(s) used.*



You can, for example, answer questionnaires or enter a progress percentage for your action plans.

Dashboard

You can add widgets adapted to various IRM issues.

See:

- [Customizing your Dashboard](#)
- [Dashboard and Widgets](#)

My Tasks

From here you can access objects of interest and on which you may have to perform an action.

See:

- [Managing Questionnaires and Check-lists](#)
- [Creating Risks and Controls](#)
- [Managing Key Indicators](#)
- [Performing a BIA \(Business Impact Analysis\)](#)
- [Taking Part in Business Continuity Plans](#)
- [Managing Action Plans and Actions](#)
- [Managing Recommendations](#)

Environment

In this section you find the objects which can populate the scope of the objects you work with.

- Business processes
- Organizational processes
- Applications
- Business lines
- Entities

For more details, see [Viewing your Environment](#).

Risks



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

This menu enables you to access:

- Your risks: the risks you own
- Risks within your scope: risks for which you are an assessor in the context of at least one of the objects of your scope

For more details on the characteristics of risks, see [Risk characteristics](#).

Controls

This menu lists all the controls for which you are responsible (for at least one of the entity in your scope).



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

For more details, see [Control Characteristics](#).

Incidents

This menu lists the incidents:

- you declared
- within your scope: incidents related to at least one object in your scope



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.

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


VIEWING YOUR ENVIRONMENT

To access the objects of your environment:

- 1 Click **Environment** then the sub-menu of interest to you.

For a detailed description of these objects, see [Managing your IRM Environment](#).


Business and organizational 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.


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

Applications

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


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

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.

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

Entities

 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.

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

DASHBOARD AND WIDGETS

Your dashboard enables you to add general or IRM-specific widgets.

To add widgets to your dashboard:

1. Click **Dashboard**.
2. Click the + sign to add a widget to your desktop.
3. Select a widget from the list.
The widget appears in your desktop.

Widgets for Action Plans

☛ *Widgets for action plans are made available in all IRM solutions.*

Action plans by progress

This pie chart presents action plan breakdown according to their progress status.

- Delayed
- On Time
- No due date
- To be due within 30 days
- Canceled
- Closed
- Delayed

Action plan by priority

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

- Critical
- High
- Mean
- Low

Action plans by status

This bar chart displays breakdown by status of actions plans you are responsible for.

- To be started
- Ongoing
- Completed

Action plan dashboard

This pie chart displays “delayed” and “on time” actions you are responsible for.

Widgets specific to IRM

Risks by status: this pie chart displays breakdown by status for risks owned by the IRM contributor.

Widgets specific HOPEX Internal Audit

See [Viewing recommendation widgets](#).

MANAGING 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.

☛ Incidents are available with **HOPEX LDC**. For more details, see [Collecting Incidents](#).

The "IRM Contributor" profile enables you to:

- Create an incident, modify it before submission or delete it.
- Analyze incidents (context and losses)
- Approve an incident that has just been declared
- Define and implement action plans

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

Creating incidents

To create an incident:

1. See [Accessing the IRM Contributor Desktop](#).
2. In the Home page, click **New Incident**.
3. Select the **Declarant's Entity**.
4. Click **Connect** then **OK**.

For more details on incidents, see the documentation for the HOPEX LDC solution. [Collecting Incidents](#).

Accessing incidents

To access your incidents:

- 】 From the desktop, click **Incidents > My incidents**.
The incidents you have created appear.

To access the incidents associated to your objects:

- 】 From the navigation menu, click **Incidents**.
- 1. The incidents of your scope are displayed.

☛ Incidents withing your scope are objects which depend on objects for which you play a specific role. You do not necessarily need to perform an action on these incidents. They are shown here for information only.

MANAGING ACTION PLANS AND ACTIONS

An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities.

☛ *Action plans are used across all IRM solutions, except in **HOPEX Internal Audit** where recommendations and actions are used instead.*

Context for action plan creation

Two types of workflows are available for action plans:

- top-down
- bottom-up

The actions that you can perform using the contributor desktop depend on the solution that you are using and the workflow implemented in your enterprise.

As a contributor, you may have to create an action plan, under different contexts, for example:

- In the "bottom-up" approach, you can create an action plan when you answer a requirement questionnaire.
☛ *You can submit it via the workflow so an approver can validate it.*
- An auditor may detect an issue and asks you to create an action plan in order to remediate it.
☛ *In this case you need to connect the issue to the action plan.*

Accessing action plans

To access action plans:

- 】 In the navigation menu, click **My Tasks > Action Plans**.

Connecting an issue to an action plan

To connect an issue to an action plan:

1. In the properties of an action plan, expand the **Scope** section and select the **Issues** tab.
2. Click **Connect**.

☛ *You can also create an issue if needed.*

Indicating action plan progress

You must indicate the progress statuses for your action plan. To do this, you can create states regularly.

To indicate progress:

1. Open the properties of the action plan.
2. Expand the **Action Plan Progress** section, and in the **Progress Update** frame, click **New**.
3. Specify a **Progress Update Percentage**.

4. Specify the progress **Evaluation**.
You can specify whether the action plan is:
 - on time, or
 - Late

Managing actions

Within the context of the internal audit or testing activities, you may, as a manager or action correspondent, be required to:


- specify the actions to take to ensure recommendation follow-up
 - ➡ See [Implementing recommendations](#).
- ensure actions are correctly implemented


To access your actions:

1. See [Accessing the IRM Contributor Desktop](#).
2. In the navigation menu, select **My tasks > Actions**.

See also [Creating an action within the framework of a recommendation](#).

MANAGING RECOMMENDATIONS

 Recommendations are used within the framework of **HOPEX Internal Audit**.

 A recommendation describes what must be done to correct noncompliance detected during an audit.

Accessing recommendations

To access your recommendations:

1. In the navigation menu, select **My tasks > Recommendations**.

Recommendations are classified according to their status:

- Recommendations
- Delayed recommendations

Implementing recommendations

You may be required to manage recommendations following testing activities or production of the final audit report.

As a recommendation owner, you may:

- create actions whose objective is to implement recommendations.
- specify a progress percentage for the actions

For more information on recommendations within the framework of **HOPEX Internal Audit**: see [Implementing Recommendations](#).

Creating an action within the framework of a recommendation

To create an action:

1. See [Accessing recommendations](#).
2. In the properties of the recommendation, select the **Action Plan** page.
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**.

 The list available in the **Owner** field corresponds to the list of auditees defined on the audit.

Submitting an action plan (consisting of recommendations)

Actions created and assigned to appropriate users constitute an action plan within the framework of **HOPEX Internal Audit**.

You may submit the action plan to the lead auditor or the audit director via the recommendations workflow.

To do this:

1. See [Accessing recommendations](#).

2. Click the recommendation name and select **Action Plan to be Submitted > Submit Action Plan.**

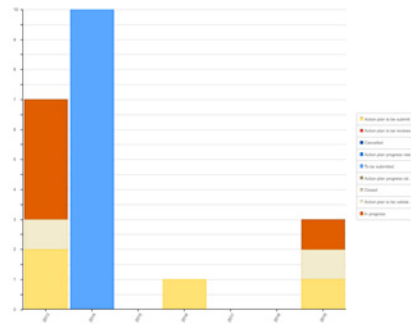
➡ The lead auditor or audit director validates the action plan by return.

Viewing recommendation widgets

Recommendations by status and year

This bar chart displays recommendations:

- By year
- By status (each color corresponding to a distinct status)



Recommendations by status and audit

This bar chart displays recommendations:

- By audit
- By status (each color corresponding to a distinct status)

Recommendation Dashboard


This dashboard displays action breakdown by progress for all “in progress” recommendations you are responsible for.

- Delayed
- On Time

MANAGING QUESTIONNAIRES AND CHECK-LISTS

An assessment questionnaire is a list of questions relating to a particular object and addressed to users.

You may be requested to complete questionnaires about controls within the framework of internal control activities.

 A check-list is a specific type of questionnaire used in **HOPEX Internal Control** for control execution.

Accessing Questionnaires

To access questionnaires:

1. See [Accessing the IRM Contributor Desktop](#).
2. In the home page, click on **My questionnaires**.

In the page that appears, the questionnaires are classified as follows:

- Questionnaires
- Late questionnaires

Answering a Questionnaire

To complete a questionnaire:


1. See [Accessing Questionnaires](#).
2. Click the questionnaire you are interested in.
3. Select the questions in turn and reply to these in the lower part of the window.
4. Click **Save**.
5. Click the questionnaire in the questionnaires list and select **Assessment Questionnaire (To Be Completed) > Submit Answers**.

After viewing the contents of a questionnaire, you can, as a respondent:


- Close the questionnaire without answering.
- Request transfer of the questionnaire to another respondent.
- Delegate all or part of a questionnaire to another person.
- Accept the questionnaire and answer.

From the questionnaire pop-up menu you can:

- Delegate all or part of a questionnaire to a third party (if, for example, you are not the person best qualified to answer certain questions).
 - Make a transfer request.
 - Close questionnaires
- Having selected the appropriate check boxes, several choices are available to the respondent:
- Save answers without sending them immediately; this allows you to return complete the questionnaire at a later time.
 - Submit the answers for validation.

 A questionnaire can be opened and closed several times before submission.

Completing Assessment Check-lists


 Check-lists are questionnaires dedicated to the HOPEX Internal Control solution and used within the context of control execution.

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

As a business user, you need to access controls in the form of check-lists.

To complete the check-lists addressed to you:


1. In the home page, click **My execution check-lists**.
2. In the list that appears, select an object to be assessed and answer the check-list questions in the lower frame.
3. Select another object to be assessed and answer the questions.
4. Click the **Save** button.
5. When you have answered all the questions, in the check-list pop-up menu, click **Automatic Assessment Questionnaire (To Be Completed) > Complete**.

 You can modify answers for as long as you do not click **Complete** in the Check-List pop-up menu.

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. 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.

 For more details on control contextualization see [Executing controls](#).

CREATING RISKS AND CONTROLS

Creating risks

To create a risk in the IRM Contributor desktop:

1. In the Home page, click **New Risk**.

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

Creating controls

To create a control in the IRM Contributor desktop:

1. In the navigation menu, select **Controls**.
2. Click **New**.

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

MANAGING KEY INDICATORS



A key indicator is a metric used by organizations to provide an early warning of increasing risk exposures in various areas of the enterprise.

Accessing Key Indicators

To access key indicators of interest/for which you need to enter a value:

- 1 In the navigation menu, select **My tasks > Indicators**.



The key indicators you can view are those for which you are requested to enter a value. See [Enter a key indicator value](#).

A list of indicators appear, with the following columns in read-only mode:

- **Current Status**
 - Pass
 - Warning
 - Unsatisfactory
 - Critical
 - Failed
- **Last Measurement (days)**: number of days elapsed since the last measurement
- **Time to Failure** (number of days)



Time to failure is the number of days before the key indicator turns to "Failed" status.

- **Value**
- **Higher Threshold** for the indicator
- **Lower Threshold** for the indicator



In the properties of a key indicator you can view advanced characteristics as well as the indicator graph.

Enter a key indicator value

To enter a key indicator value:

1. See [Accessing Key Indicators](#).
2. Open the the properties of a key indicator and select the **Values** tab.
3. In the **Values** section, click **New**.
4. Enter a value and click **OK**.

Submitting an action plan on a key indicator

To create and submit an action plan:

1. See [Accessing Key Indicators](#).
2. Open the the properties of a key indicator and select the **Action Plans** tab.
3. Click **New** to enter a comment as well as forecast dates.
4. Roll the mouse over the action plan action and select **To be Submitted > Submit**.

5. Enter a comment and click **OK**.

PERFORMING A BIA (BUSINESS IMPACT ANALYSIS)

As a contributor, you can perform a BIA (Business Impact Analysis).

 This feature is available with **HOPEX BCM**.

To access a BIA that have been sent to you:

1. In the navigation menu, click **My tasks > Business Continuity**.
2. Expand the **Business Impact Analyses** section.
All the BIAs that have been assigned to you appear here. The BIAs that you have closed are also listed here so that you could reopen them if needed.
3. Open the properties of the BIA of interest.
4. Answer the questions in the section containing the BIA matrix.
5. Click the **Complete** button.


TAKING PART IN BUSINESS CONTINUITY PLANS

As a contributor, you may be asked to take part in Business Continuity Plans.

 This feature is available with **HOPEX BCM**.

You may be asked to manage recovery steps within the framework of:

- Business continuity exercises
- Crises

 Recovery steps must be implemented within the framework of specific Business Continuity Plans.

Viewing BCPs tested by ongoing exercises

You may be asked to take part in Business Continuity Plan testing within the framework of ongoing exercises.

To view these:

1. In the navigation menu, click **My tasks > Business Continuity**.
2. Expand the **Business Continuity Plans tested by ongoing exercises**

This list displays BCPs tested within the framework of an ongoing business continuity exercise.

Viewing BCPs triggered by ongoing crises

You may be asked to take part in Business Continuity Plan execution within the framework of crises.

To view these:


1. In the navigation menu:
 - (HOPEX IRM) Select **My tasks > Business continuity**.
 - (HOPEX Business Process Analysis) Select **Continuity > Continuity tasks**.
2. Expand the **Business Continuity Plans triggered by ongoing crises**.

This list displays BCPs triggered within the framework of an ongoing crisis.



APPENDIX - COMPUTATION RULES

Risk Control Level

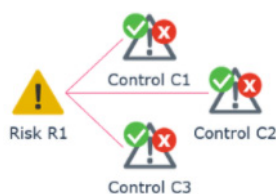
 Risk control level enables characterization of control efficiency in mitigating the risk.

Context

When a respondent completes a risk assessment questionnaire, **HOPEX IRM** displays a value for Control Level.

A value is displayed if:

- the risk is mitigated by one or several controls.
- controls mitigating the risk have already been assessed (and therefore shows a value for aggregated control level).



Computation method

The computation method consists of two steps:

1) Computation of control level average

$$\text{Average Control Level} = \frac{\text{Total nb. of deficient controls} \times 25}{\text{Total number of controls}}$$

2) Mapping the obtained result (rounded off to the next integer) with the Control Level internal values

Control level (On Risk)	Internal value
Effective	1
Few observations	4
Frequent observations	9
Ineffective	16
Inexistent	25

☛ The displayed Risk Control level corresponds to the internal value which is closest to the previously computed average.

Example: Risk Control Level displays "Frequent observations" if control level average = 10.

Computation example

Control	Aggregated Control Level	Control Level value
C1	90%	1
C2	45%	0
C3	0%	0

Control Level average = $2 \times 25 / 3 = 16,6$ -> rounded off to 17.

☛ C2 and C3 controls are considered to be "failed" (because < 90%).

Risk Control Level is considered ineffective (because 16 is the internal value closest to 17).

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.

Computation method

Inherent risk = Impact x Likelihood

Possible values

- Very Low (1)
- Low (4)
- Medium (9)
- High (16)
- Very High (25)

Impact	5	Very High	5	10	15	20	25
	4	High	4	8	12	16	20
	3	Medium	3	6	9	12	15
	2	Low	2	4	6	8	10
	1	Very Low	1	2	3	4	5
			Rare	Possible	Likely	Probable	Certain
			1	2	3	4	5
			Likelihood				

Residual Risk

The residual (or net risk) indicates the risk to which the organization remains exposed after management has processed the risk.

Computation method

The residual risk is computed based on the inherent risk (Impact * Likelihood) and the control risk level.

Possible values

- Very Low (1)
- Low (16)
- Medium (81)
- High (256)
- Very High (625)

Inherent Risk	Very High	Medium	Medium	High	High	Very High
	High	Low	Medium	Medium	High	High
	Medium	Low	Low	Medium	Medium	Medium
	Low	Very Low	Low	Low	Low	Low
	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
Control Level						

RTO (Recovery Time Objective) Computation



The RTO (Recovery Time Objective) is the time frame identified for resuming disrupted activities.



For more details, see [Viewing BIA Computed Results](#).

The algorithm:

- adds up of the weights of the impact types answers for every downtime period, from the smallest downtime period to the highest
- compares this sum with the RTO Threshold.

The RTO Threshold is defined for every downtime period. It consists of the maximum possible values that the BIA answers can have minus 30%.

The computed RTO is the downtime period for which the sum of the answer values is higher than the RTO Threshold.

Max values (« Critical »)

	12 Hours	INT VALUE	1 Day	INT VALUE	2 Days	INT VALUE	1 Week	INT VALUE	2 Weeks	INT VALUE	1 Month	INT VALUE
Financial	F-Critical	16	F-Critical	16	F-Critical	16	F-Critical	16	F-Critical	16	F-Critical	16
Operational	O-Critical	12	O-Critical	12	O-Critical	12	O-Critical	12	O-Critical	12	O-Critical	12
Environmental	E-Critical	8	E-Critical	8	E-Critical	8	E-Critical	8	E-Critical	8	E-Critical	8
Reputational	R-Critical	4	R-Critical	4	R-Critical	4	R-Critical	4	R-Critical	4	R-Critical	4
Sum		40		40		40		40		40		40

RTO Threshold (for each downtime period) = Sum of maximum values - 30%
 Example (standard business continuity analysis template) : $40 - 30\% = 28$

1		12 Hours	INT VALUE	1 Day	INT VALUE
2	Financial	F-Medium	8	F-High	12
3	Operational	O-High	9	O-High	9
4	Environmental	E-High	6	E-High	6
5	Reputational	R-Medium	2	R-Medium	2
			25		29

29 is higher than the standard RTO threshold
 -> RTO = 1 day

Business Impact Computation

The business impact is computed from the answers given in the BIA matrix.

➡ For more details, see [Defining a Business Impact Analysis](#).

The business impact is computed as follows:

If RTO = Business impact =
12 hours or 1 day	Critical
2 days or one week	Medium
Other values	Low



IRM GLOSSARY



action



An action is included in an action plan and represents a transformation or processing in an organization or system.

action plan



An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities.

activity program

An activity program is an activity template relating to the main characteristics of an audit activity to be carried out.

aggregation method

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

aggregation period

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

aggregation rule

An aggregation rule handles calculation of values for a parent assessment characteristic from one or several child assessment characteristics. A few rules are defined by default, for instance: max, min, sum, average

aggregation schema

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

application



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

article (of regulatory framework)

An article is a citation from a regulatory framework and is usually associated to a mandated control directive.

**assessed characteristic**

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.

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 campaign

An assessment campaign enables creation and planning of several assessment sessions over a given time period.

assessment freshness

Assessment freshness is the number of days elapsed since an indicator value was last entered.

assessment session

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 template

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

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

audit

An audit is a mission assigned to an internal auditor in the context of an audit plan.

**audit activity**

An audit activity is an element of an audit that can relate to a set of processes, applications, risks or controls to be audited in an enterprise organization unit.

**audit program**

An audit program is a template relating to the main characteristics of an audit.

audit theme

An audit theme is a collection of audit activities dealing with the same topic. Audit themes consist of sub-audit themes.

business document

A business document is a document whose content is independent from the HOPEX 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.

business line

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.

business policy

A business policy is an internal document issued by an organization (security measure, best practice, etc.).

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.

calendar

A calendar is divided into calendar periods.

calendar

A calendar is divided into time periods called calendar periods. Calendars can be used in assessment campaigns, in report generation as well as to schedule audits/tests.

calendar period

A calendar period is a division of a calendar.

central currency

Central currency is the currency adopted as reference currency.

company

A company is a legal entity.

compliance rate

The compliance rate is the percentage of "Pass" controls.

control

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

control assessor

The Control assessor is responsible for assessing and executing controls within his/her scope, as well as implementing action plans related to these controls.

control directive

Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

risk control level

Risk control level enables characterization of control efficiency in mitigating the risk.

control level

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

Control level is the percentage of assessment nodes (objects assessed in each context for each respondent) that obtained "Pass" during the last assessment (direct or by campaign).

control redundancy

A control redundancy formalizes the fact that several controls are redundant. This can be, for example, because they have been successively installed to cover the same risk in the contexts of different regulations.

control type

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

database

A database enables specification of data logical or physical storage structure.

department

An organization unit (org-unit) is an element of the enterprise structure such as a department or a service. It is defined based on how detailed you require your view of the enterprise to be. Example: financial management, sales management, marketing department, account manager.

enterprise stage

An enterprise stage is a past, current or future stage of an enterprise.

entity

An org-unit represents a person or a group of persons that intervenes in the enterprise business processes or information system.

entity

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.

execution rate

The execution rate is the percentage of objects in the control scope that were included in the last control execution campaign.

findings

Audit findings are the results of assessment of the collected audit evidence against audit criteria. Audit findings can indicate either conformity or nonconformity with audit criteria or opportunities for improvement.

forecast risk

Forecast risk represents the residual risk forecast for the year to come.

gain

A gain is the positive financial consequence of an incident.

**incident**

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.

incident approver

Incident approver is the role used in standard workflows to approve incidents.

incident declarant

The incident declarant is in charge of creating incidents within his/her scope.

indicator

An indicator is a measure of achievement of an objective, impact of a risk factor, frequency and impact of a risk, effectiveness of a control, etc.

indicator interpretation logic

An indicator interpretation logic contains the logic behind the computation of the indicator status, Time to Failure, together with the list of possible statuses for the indicator.

Indicator status

The status of an indicator enables to define whether an alert must be triggered. An indicator is computed automatically based on the latest indicator values, the aggregation period and the aggregation method.

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.

internal audit

Internal audit is an independent and objective activity assuring an organization on the degree of control of its operations, proposing recommendations for their improvement, and contributing to added value. It helps an organization achieve its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (source: IIA).

key indicator

A key indicator is a metric used by organizations to provide an early warning of increasing risk exposures in various areas of the enterprise.

Key Indicator Category

The key indicator category enables to specify how indicator values are interpreted, in order to compute the indicator status and Time to Failure.

library

Libraries are collections of objects used to split HOPEX repository content into several independent parts. Two objects owned by different libraries can have the same name.

local currency

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

loss

A loss is the negative financial result of an event.



macro-incident

A macro-incident is an event that impacts more than one business or company of the same group.

**materialized risk**

A materialized risk is a risk for which an incident occurred.

metric

A metric provides quantitative indications on value of a measurement (for example risk prevention level).

near-miss

A near-miss is an incident that did not result in injury, illness, or damage - but had the potential to do so.

objective

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

operation

An operation is an elementary step in an organizational process. It corresponds to the intervention of an entity withing the organization.

organizational processes

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

**period**

A period corresponds to the fiscal period over which audits are carried out. It enables chronological grouping of several audit plans.

person

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.

policy framework

A policy framework consists of a set of business policies. Policy frameworks may contain sections.

**product**

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.

profile

A profile defines access to application functions, as well as the level of intervention in the workflow and validation process.

provision

A provision is an amount deducted from the result to cover risks or unexpected charges. Several provisions can concern a single risk.

**questionnaire**

An assessment questionnaire is a list of questions relating to a particular object and addressed to users.

questionnaire template

A questionnaire template represents definition of questionnaire content.

recommendation

A recommendation describes what must be done to correct noncompliance detected during an audit.

**recovery**

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.

**regulation framework**

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.

regulation or policy

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.

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), or standards.

**requirement**

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.

residual risk

The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

respondent

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.

risk

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

**risk and control system**

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.

risk appetite

Risk appetite is the level of risk an organization is ready to accept to reach its objectives, before any measure is taken to mitigate the risk.

Risk assessor

The Risk assessor is responsible for assessing risks within his scope, as well as implementing action plans related to these risks.

risk consequence

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

**risk factor**

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 Manager

The Risk Manager is responsible for executing the following tasks on risks within his/her responsibility domain: identify risks, perform direct assessments, manage assessment campaigns, define action plans, analyze and follow report creation.

Risk type

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

**role**

A role is the association of a profile with a user in a specific organizational context.

scoring rule

Scoring rules indicate how the answers to a questionnaire populate the characteristics of assessed objects.

section (of regulatory framework)

A section is a citation from a regulatory framework without any mandated control directive, but containing other sections or articles.

**server**

A computer which provides a service to the users connected to it via a network. This computer can have a database and run Applications.

steering calendar

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

test

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



test plan

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.

Time to Failure

Time to failure is the number of days before the key indicator turns to "Failed" status.

workpaper

A workpaper comprises points to be checked on a given subject in the course of an audit activity.

HOPEX Internal Control



HOPEX Internal Control

User Guide

HOPEX V5



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 is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2021

All rights reserved.

HOPEX Internal Control and HOPEX are 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.

CONTENTS



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

About Control Management	9
---	----------

Internal Control Process.	10
<i>Control register definition</i>	<i>10</i>
<i>Control Execution</i>	<i>10</i>
<i>Control Assessment</i>	<i>11</i>
<i>Issue and Action Plan Management</i>	<i>11</i>
Control Management Profiles	12

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

Creating Controls	14
------------------------------------	-----------

Control Characteristics	15
--	-----------

General characteristics	15
<i>Code</i>	<i>15</i>
<i>Key control</i>	<i>15</i>
<i>Status</i>	<i>15</i>
<i>Owner</i>	<i>15</i>
<i>Control nature.</i>	<i>15</i>
<i>Execution mode.</i>	<i>15</i>
<i>Operational cost</i>	<i>15</i>
<i>Description</i>	<i>16</i>
Control Dashboard	16
<i>Last assessment</i>	<i>16</i>
<i>Last compliance rate</i>	<i>16</i>
<i>Open issues</i>	<i>16</i>
<i>Control level</i>	<i>16</i>
Responsibilities concerning Controls	16

<i>Responsibility levels</i>	17
<i>Specifying control responsible users</i>	17
Scope of a Control and Associated Risks	18
Regulatory and Business Policy Enforcement	18
Action Plans for Controls	18
Reports Related to Controls	19
Accessing Controls	20
Listing Controls	20
Accessing Orphan Controls	20
Accessing Controls by Incidents	21
Contextualizing Controls	22

Assessing controls **23**

Control Assessment Types	24
Direct Assessment or by Campaign	24
<i>Direct assessment</i>	24
<i>Evaluation By Campaign</i>	24
Available Assessment Templates	24
Pre-requisites to Control Assessment	25
Control Assessment by Entity	25
<i>Assessment contexts</i>	25
<i>Prerequisites</i>	25
<i>Respondent definition logics</i>	25
<i>Specifying respondents</i>	26
Control Assessment by Entity and Regulatory Framework	26
<i>Assessment contexts</i>	26
<i>Prerequisites</i>	27
<i>Possible use</i>	28
Control Direct Assessment	29
Direct Assessment Context	29
Assessing a Control	29
Assessing Multiple Controls Simultaneously	30
Assessment Control Results	32
Displaying the Results of Control Assessment.	32
Analyzing Control Assessment Results	32
<i>Instant reports</i>	32
<i>Dedicated analysis reports</i>	33
Assessment Result Computing Mode	33

Executing controls **35**

Preparing Control Execution	36
Defining Questions on Controls	36
Defining Steering Calendars on Controls	36
<i>Specifying a control steering calendar</i>	36

<i>Modifying a steering calendar after campaign creation</i>	37
Defining the Total Population and Sample Size	37
Defining Respondents	38
Connecting Controls to Entity Processes	38
Continuous Control Assessment Template	39
<i>Respondents</i>	39
<i>Check-lists sent</i>	39
<i>Answer computation</i>	39
<i>Aggregated results</i>	39
Creating Execution Campaigns	40
Defining scope via a tree	40
Displaying the Execution Campaign Summary	41
<i>General information (Overview)</i>	41
<i>Contexts</i>	42
<i>Respondents</i>	42
<i>Assessed objects</i>	42
How an Execution Campaign Works	43
Control Execution Periodicity	43
Examples of Session Automatic Launch	43
Consulting Execution Campaign Schedule	44
Defining Reminders	44
<i>Modifying reminders provided as standard</i>	44
<i>Deactivating reminders</i>	45
Closing Check-lists	45
Completing Control Execution Check-Lists	46
Completing a Check-List	46
Transferring a Check-List	46
Managing Execution Check-Lists	47
Accessing Check-Lists	47
Reassigning Check-Lists	47
Check-List Results	48
Control Execution Reports	49
Detailed Execution Results	49
<i>Access path</i>	49
<i>Parameters</i>	49
<i>Result</i>	49
Consolidated Execution Results	49
<i>Access path</i>	49
<i>Parameters</i>	50
<i>Result</i>	50
Following Up Execution Sessions	50
<i>Access path</i>	50
<i>Availability</i>	50
<i>Parameters</i>	51
<i>Result</i>	51

Managing Compliance	53
About Unified Compliance Framework	54
Main UCF Concepts	54
<i>Authority Documents</i>	54
<i>Citations</i>	54
<i>UCF Controls</i>	54
<i>Links between UCF concepts</i>	55
<i>Building a Shared List</i>	55
Mapping between UCF and HOPEX Concepts	56
Managing the Regulatory Environment	57
Using UCF Import	57
<i>UCF Import Prerequisites</i>	57
<i>Parameterizing UCF Import</i>	57
<i>Importing Data from the Common Controls Hub</i>	58
Defining the Applicable Regulatory Content	58
<i>Regulatory content relevance</i>	58
<i>Reviewing regulatory frameworks after UCF import</i>	59
<i>Selecting relevant content for your organization</i>	59
Managing the Compliance Register	60
Concepts Used in the Compliance Register	60
Accessing the Elements of the Compliance Register	60
<i>Displaying elements as a list</i>	61
<i>Displaying control directives in a tree of regulatory frameworks</i>	61
<i>Displaying business policies in a tree</i>	61
Viewing Regulatory Frameworks	62
<i>Accessing regulatory frameworks</i>	62
<i>Regulatory framework overview & description</i>	63
<i>Content of a regulatory framework</i>	63
Viewing Regulation Articles	64
<i>Accessing regulation articles</i>	64
<i>Connecting or viewing objects subjected to a regulation article</i>	64
<i>Enforcement of a regulatory article</i>	65
<i>Connecting Business Documents</i>	65
Viewing Control Directives	66
<i>Accessing control directives</i>	66
<i>Viewing articles associated to a control directive</i>	66
<i>Supported and supporting directives</i>	67
<i>Enforcement level of control directives</i>	68
<i>Viewing HOPEX controls implementing a control directive</i>	68
<i>Attaching business documents or external references</i>	69
IT Regulatory Compliance Reports	70
Regulatory Compliance by Entity	70
<i>Access path</i>	70
<i>Parameters and Launch</i>	70
<i>Example</i>	72
Regulatory Framework Implementation	73
<i>Access path</i>	73
<i>Parameters</i>	73
<i>Results</i>	73
Compliance by Regulatory Framework	74

<i>Access path</i>	74
<i>Parameters</i>	74
<i>Results</i>	74
Regulatory Compliance Overview	75
<i>Access path</i>	75
<i>Parameters</i>	75
<i>Results</i>	75
Regulatory Compliance Progress	76
<i>Access path</i>	76
<i>Parameters</i>	76
<i>Report example</i>	76

Control Testing 77

Preparing Control Testing 78

Defining Test Sheet Questions	78
Defining Testing Methods	78

Preparing Tests 79

Creating Test Plans	79
Planning Tests	80
<i>Accessing tests</i>	80
<i>Publishing tests</i>	86
Preparing Tests	86
<i>Work program creation prerequisites</i>	86
<i>Work program content</i>	87
<i>Creating work programs automatically</i>	87
<i>Completing the work program manually</i>	88

Executing Tests 93

Consulting the Work Program	93
Executing Tests on Samples	93
<i>Creating workpapers</i>	93
<i>Specifying or modifying the sample size</i>	94
<i>Generating the test sample</i>	94
<i>Defining test sheet questions</i>	94
<i>Completing the generated test sheets</i>	95
<i>Assessing test activities</i>	95
Assessing Controls	95
<i>Generating questionnaires</i>	95
<i>Responding to Questionnaires</i>	95
Managing Time and Expenses	96
<i>Managing Expenses</i>	96
<i>Entering Vacations</i>	97
<i>Completing a Time Sheet</i>	97
Management of issues and action plans	97
<i>Managing issues</i>	98
<i>Managing Action Plans</i>	98
Supervising Tests	99
<i>Test check reports</i>	99
<i>Time Sheet Follow-up Reports</i>	99

<i>Test expenses reports</i>	100
Concluding Tests	100
<i>Test assessment reports</i>	100
<i>Generating test reports</i>	100
<i>Assessing tests</i>	100
<i>Terminating tests</i>	101
<i>Closing tests</i>	101
Test Follow-Up	102
Implementing Action Plans	102
<i>Accessing action plans</i>	102
<i>Implementing actions</i>	102
<i>Action plan implementation follow-up</i>	102
<i>Action Plan Follow-Up</i>	103
Test Plan Follow-Up	103
<i>Displaying test plan follow-up reports</i>	103
<i>Closing a test plan</i>	104
Testing Dashboard	104
<hr/>	
Managing Issues and Action Plans	107
Managing issues	108
Creating Issues	108
Scoping an Issue	108
Remediating Issues	108
Following-Up Issues	108
<i>Viewing remediated / non-remediated issues</i>	108
<i>Generating issue follow-up reports</i>	109
Managing Action Plans	110
Accessing action plans	110
Creating an Action Plan for Testing	110
Characterizing Action Plans	110
<i>Action Plan Dashboard</i>	111
<i>General characteristics</i>	112
<i>Responsibilities</i>	112
<i>Financial assertion</i>	113
<i>Success Factors and Outcome</i>	113
<i>Scope</i>	113
<i>Progress history</i>	113
<i>Milestones</i>	113
<i>Attachments</i>	113
Managing Actions	114
<i>Creating actions</i>	114
Action Plan Workflows	114
<i>"Bottom-up" approach</i>	114
<i>"Top-down" approach</i>	115
<i>Action workflow</i>	115
Indicating Action Plan Progress	115
Action plan follow-up reports	115
<i>Access path</i>	116

<i>Result</i>	116
-------------------------	-----

Reports Related to Controls 119

Control Environment Report 120

<i>Access path</i>	120
------------------------------	-----

<i>Report parameters</i>	120
------------------------------------	-----

<i>Creating a control environment report</i>	121
--	-----

<i>Example</i>	121
--------------------------	-----

Control Register Reports 122

Control Identification	122
----------------------------------	-----

<i>Access path</i>	122
------------------------------	-----

<i>Parameters</i>	122
-----------------------------	-----

<i>Results</i>	123
--------------------------	-----

<i>Example</i>	123
--------------------------	-----

Control Location Matrix	124
-----------------------------------	-----

<i>Access path</i>	124
------------------------------	-----

<i>Parameters</i>	124
-----------------------------	-----

<i>Example</i>	124
--------------------------	-----

Control Execution Reports 125

Detailed Execution Results	125
--------------------------------------	-----

<i>Access path</i>	125
------------------------------	-----

<i>Parameters</i>	125
-----------------------------	-----

<i>Result and example</i>	126
-------------------------------------	-----

Consolidated Execution Results	126
--	-----

<i>Access path</i>	126
------------------------------	-----

<i>Parameters</i>	127
-----------------------------	-----

<i>Result</i>	127
-------------------------	-----

<i>Example</i>	128
--------------------------	-----

Following Up Execution Sessions	128
---	-----

<i>Access path</i>	128
------------------------------	-----

<i>Availability</i>	128
-------------------------------	-----

<i>Parameters</i>	128
-----------------------------	-----

<i>Result</i>	128
-------------------------	-----

Control Assessment Reports 130

Campaign Result Tree	130
--------------------------------	-----

<i>Access path</i>	130
------------------------------	-----

<i>Parameters</i>	130
-----------------------------	-----

Campaign Result Matrix By Entity	130
--	-----

<i>Access path</i>	130
------------------------------	-----

<i>Parameters</i>	130
-----------------------------	-----

<i>Example</i>	131
--------------------------	-----

Aggregation Report	131
------------------------------	-----

<i>Access path</i>	131
------------------------------	-----

<i>Parameters</i>	132
-----------------------------	-----

Control Assessment Follow-Up Reports 133

Session Follow-Up	133
-----------------------------	-----

<i>Access path</i>	133
------------------------------	-----

<i>Parameters</i>	133
-----------------------------	-----

<i>Result</i>	133
Session Statistics	133
<i>Access path</i>	133
<i>Parameters</i>	134
<i>Result</i>	134
<i>Report example</i>	134
Failed Controls	135
<i>Access path</i>	135
<i>Parameters</i>	135
<i>Result</i>	135
<i>Report example</i>	135
Control Testing Reports	136
Testing Coverage	136
Plan Synthesis	136
<i>Access path</i>	136
<i>Result</i>	136
<i>Example</i>	137
Other Reports.	137
<i>Test plan follow-up reports</i>	137
<i>Test follow-up report</i>	137
<i>Action plan report.</i>	137
Issue-Related Reports	138
Issue Follow-up Report	138
<i>Access path</i>	138
<i>Result</i>	138
<i>Example</i>	138
"Issues by Impact" Report	139
<i>Access path</i>	139
<i>Result</i>	139

ABOUT CONTROL MANAGEMENT



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

- ✓ definition of internal controls with creation of a control register
- ✓ execution of controls
- ✓ assessment of controls, directly or by assessment campaigns or tests
- ✓ management of your regulatory library and IT compliance implementation
- ✓ management of issues and action plans

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

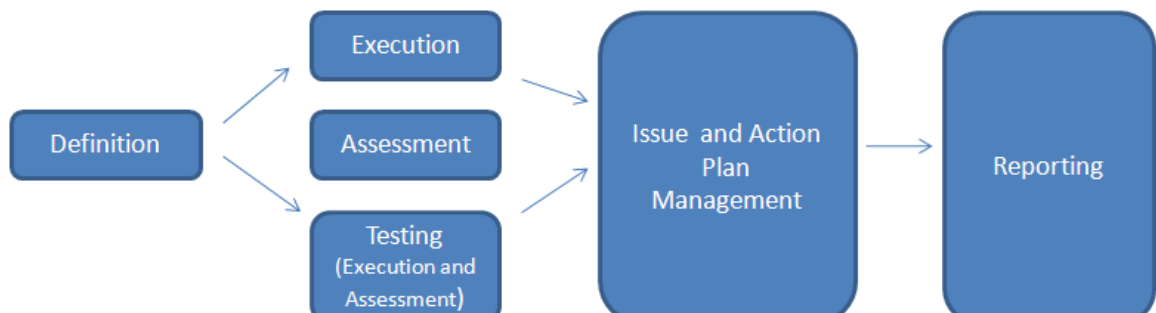
- ✓ [Internal Control Process](#)
- ✓ [Control Management Profiles](#)

INTERNAL CONTROL PROCESS

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

HOPEX IRM 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 register definition

HOPEX IRM 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 IRM** 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 IRM** 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](#).

CONTROL MANAGEMENT PROFILES

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

Profiles	Desktop	Tasks
Internal Control Director (or IRM 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 IRM 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
IRM Contributor	IRM Contributors	<p>Use the simplified HOPEX Explorer desktop.</p> <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>

➡ For more details, see [Accessing the IRM Manager Desktop](#).

MANAGING CONTROLS



HOPEX IRM enables creation of control registers 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.

- ✓ [Creating Controls](#)
- ✓ [Control Characteristics](#)
- ✓ [Accessing Controls](#)
- ✓ [Contextualizing Controls](#)

CREATING CONTROLS

To create a control:

1. In the **HOPEX IRM** desktop, select **Registers > Controls > All Controls**.
2. Click **New**.
3. In the creation wizard, enter:
 - the **Name**
 - **Control Nature**
 - **Execution Mode**
 - a **Description**.

➡ For more details on characteristics, see [Control Characteristics](#).

The control created appears in the list of controls.

You can specify the various characteristics from the properties page.

CONTROL CHARACTERISTICS

➡ To access controls, see [Accessing Controls](#).

General characteristics

Code

The code enables unique identification of the control.

Key control

Status

- Draft
- Validated

➡ Status must be entered manually.

Owner

The control owner is by default the control creator.

➡ The control owner has no particular task to perform.

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

Execution mode

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

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

Operational cost

This characteristic enables indication of a control cost assessment.

Description

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

Control Dashboard

See also: [Accessing Controls](#).


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

Last assessment

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

Last compliance rate

The compliance rate relates to control execution check-lists. For more details on this functionality, see [Executing controls](#).

 *The compliance rate is the percentage of "Pass" controls.*

Open issues

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

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

Control level

Control Level is related to control assessment. For more details, see [Displaying the Results of Control Assessment](#).

Control level is the percentage of assessment nodes (objects assessed in each context for each respondent) that obtained "Pass" during the last direct assessment or assessment campaign.

If a control is being assessed in 2 contexts (for example 2 business processes) and that one of the assessment "Pass" the control level is 50%.

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

Responsibilities concerning Controls

See also: [Accessing Controls](#).

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

- Responsible
- Accountable
- Consulted
- Informed

Responsibility levels

RACI responsibility levels are as follows:

Responsibility	Explanation
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 and execution, questionnaire respondents are **Responsible** users of the control.

☛ See the section corresponding to the respondent logics in the prerequisites to control assessment. [Pre-requisites to Control Assessment](#).

☛ See also: [Managing Assessment Campaigns](#).

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 **New** button.
4. Select a person in the drop-down list provided.
 - ☛ The business role "Control Responsible" is specified by default.
5. (optional) Select the entity the person is responsible for.
6. Click **OK**.

☛ Ensure that an e-mail address is correctly specified next to the name of the person.

☛ You have the possibility to connect several responsible users.

Scope of a Control and Associated Risks

To specify the scope of a control:

- 1 In the control properties, expand the **Scope** section.
You can connect several object types:
 - Business processes
 - Organizational processes
 - Operations
 - Entities
 - Applications
 - Accounts
 - Types of control

To specify risks for a control:




- 1 In the control properties, expand the **Risks** section.

Regulatory and Business Policy Enforcement

To view regulatory and business policy elements that are connected to a control:

1. See [Accessing Controls](#).
2. In the properties of a control, expand the **Regulatory and Policy Enforcement** section.

Several tabs enable you to view associated objects:


- Control Directives
 -  *Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.*
- Articles
 -  *An article is a citation from a regulatory framework and is usually associated to a mandated control directive.*
- Business Policies
 -  *For more details, see [Managing Compliance](#).*

Action Plans for Controls

To specify action plans on a control:

- 1 In the control properties, select the **Action plans** page.

You can:

- define action plans directly on the control
- view action plans on issues associated to the control
 -  *For more details, see [Managing Issues and Action Plans](#).*

Reports Related to Controls

See [Control Environment Report](#).

ACCESSING CONTROLS

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

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.

Listing Controls

To list all controls:

- 】 In the **HOPEX IRM** desktop, select **Registers > Controls > All Controls**.

For each control, you can access the following information:

- **Code**
- **Key control** (is it a key control or not?)
- Associated business or organizational **Processes** (connected directly or via a risk connected to a the control)
- **Last Assessment** (date)
- **Issues** (number of)
- **Nature**
- **Execution mode**
- **Execution frequency**

☛ *You may use these columns to sort controls according to different criteria, or add other columns.*

Accessing Orphan Controls

To access controls that mitigate no risks and are not connected to any element of the organization:

- 】 In the **HOPEX IRM** desktop, select **Registers > Controls > Orphan Controls**.


To define a control in a proper way:

- 】 Connect it to a risk and make sure you have defined the risk scope.

Accessing Controls by Incidents

To access controls that mitigate risks materialized by one or several incidents:

- 1 In the **HOPEX IRM** desktop, select **Registers > Controls > Controls by Incidents**.

 A risk is considered as materialized when it is connected to an incident that is in a status other than Draft or Rejected.

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 risks that are connected to processes or entities**.

☛ You may also **connect controls to entities via the indirect link "Control->Process->Entity"**, which means:

- Connect processes (organizational or business) to entities of the organization.
- Connect controls to processes

ASSESSING CONTROLS



Controls are assessed in terms of design/efficiency.

Assessment can be made:

- Directly on controls (assessment by an expert)
- Via questionnaires (IRM Contributor)

HOPEX IRM also enables internal controllers and auditors to answer questionnaires on site. For more details, see [Control Testing](#).

☛ *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](#).*

- ✓ [Control Assessment Types](#)
- ✓ [Control Assessment by Entity](#)
- ✓ [Control Assessment by Entity and Regulatory Framework](#)
- ✓ [Control Direct Assessment](#)
- ✓ [Displaying the Results of Control Assessment](#)

CONTROL ASSESSMENT TYPES

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

Direct Assessment or by Campaign

Direct assessment

The IRM Manager can specify characteristic values:

- From the control properties page: see [Assessing a Control](#).
- From a multiple assessment table: see [Assessing Multiple Controls Simultaneously](#).



Evaluation By Campaign

Characteristic values can be collected via an assessment questionnaire sent to appropriate recipients: see [Starting an Assessment Campaign](#)

Available Assessment Templates

HOPEX enables you to assess controls from two different perspectives:

- [Control Assessment by Entity](#)
- [Control Assessment by Entity and Regulatory Framework](#).

☛ See [Pre-requisites to Control Assessment](#) for more information on these assessment templates.

PRE-REQUISITES TO CONTROL ASSESSMENT

Control Assessment by Entity

The template “Control Assessment” enables to assess control in the context of entities and business/organizational processes based on the following criteria:

- Design
- Effectiveness

Assessment contexts

Controls are assessed in the context of entities, processes and operations.

Prerequisites

Before starting control assessment, you must first prepare the work environment.

Check that you have:

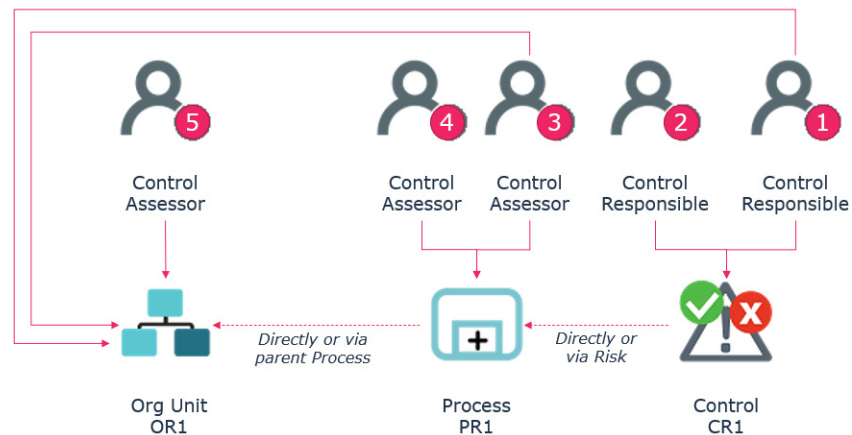
- connected controls to processes (indirectly via risks, or directly)
- connected processes to the organization entities (directly or indirectly via the parent process)
 - See [Contextualizing Controls](#).
- defined respondents.
 - See:
 - [Pre-requisites to Control Assessment](#)
 - [Specifying respondents](#)
- specified an e-mail for each respondent.

Respondent definition logics

Respondents to control-related questionnaires can be defined on:

- entities
- controls connected to entities (via a risk or indirectly via the parent process)
- controls connected to processes (via a risk or directly)
 - See also [Contextualizing Controls](#).

Hereafter the logical order used to compute respondents on controls:



The control respondent is computed in the following order:

1. A control responsible located on an entity
2. A control responsible without any localization
3. A control assessor on a process with localization
4. A control assessor on a process with localization
5. A control assessor on an entity

Specifying respondents

To specify respondents, see:

- [Specifying control responsible users.](#)
- [Specifying process responsibilities](#)
- [Specifying responsibilities within an entity](#)

Control Assessment by Entity and Regulatory Framework

The assessment template “Control assessment by entity and regulatory framework” enables to assess the organization IT compliance with applicable regulations.

Assessment contexts

Controls are assessed in the context of processes and applications.

The assessed controls are connected to a control directive of a regulatory framework impacting:

- a process directly or indirectly connected to the entity
- an application connected to a process, which is directly or indirectly connected to the entity

Controls are to be selected in the following tree: **Regulatory Framework > Control directive > Context (application or process) > Control**

✓	NIST Framework			
✓	Change default passwords			
✓	Control 1			
✓	Application 1			
✓	Install all security patches			
✓	Control 2			
✓	Application 1			
✓	Org Process 1			

☛ Controls can be connected to risks, which are connected to applications or processes.

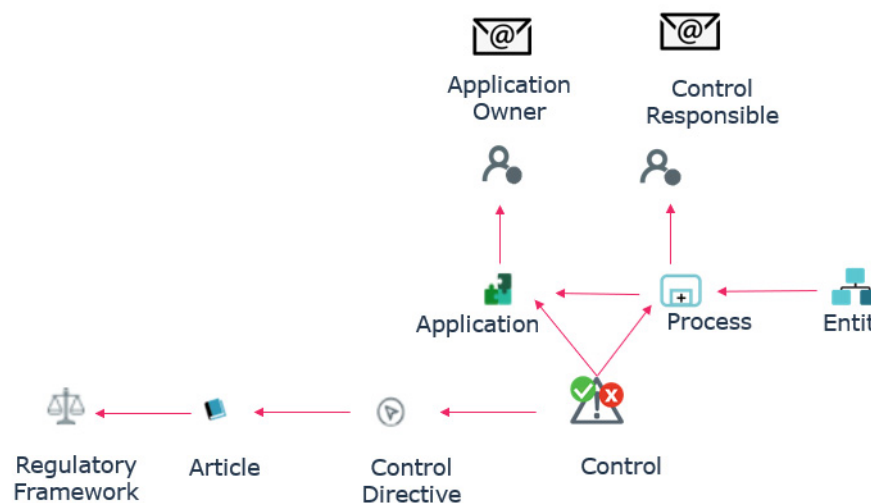
☛ Controls connected to an application non connected to a process are excluded.

Prerequisites

Check that you have:

- connected controls to control directives.
- connected controls to processes or applications.
- defined respondents.
 - for applications: the application owner
 - For processes: the control responsible user
- specified an e-mail for each respondent.

☛ See [Specifying process responsibilities](#).



Possible use

This assessment template can be used with the framework of:

- control assessment campaigns
- multiple direct assessment

☛ *Specific reports enable to follow-up the compliance process progress. See [IT Regulatory Compliance Reports](#).*

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](#).
 - ☛ See also: [Pre-requisites to Control Assessment](#).

Direct Assessment Context

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

- in the properties of each control: [Assessing a Control](#).
- globally: [Assessing Multiple Controls Simultaneously](#)

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
- Operations
- Entities
- Applications

☛ 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**.
 - ☛ If the control has not been properly contextualized, a warning is displayed (a control must be connected to a process, in turn 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 **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).

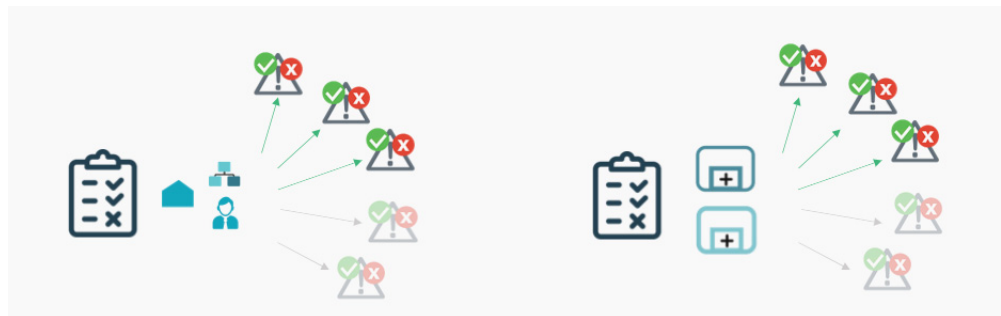
You can create several measures on different dates in the same way.

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 Table Assessment Table**.
2. Click **Launch Multiple Assessment**.

3. In the window that appears, select the assessment template:
 - "Control Assessment"
 - "Control Assessment by Entity and Regulatory Framework"

 For more details, see [Available Assessment Templates](#).



















4. In the displayed tree, select the context objects of interest.

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


The following Information is given in columns to help you select the controls to assess:

- **Last assessment**
- **Open issues**
- **Control level**

 This information is also available in the control dashboard. For more details, see [Accessing Controls](#).

	Assessment Freshness	Open Issues	Aggregated Pass Control Level
  MyCompanya			
  World@Hand Corporation			
  Regional Headquater			
  HR Department			
  Develop and Manage Human Capitala			
  Manage HR Administration and Payrolla			
  Manage Skills and Competences			
  Control on special orders	73 months	2	100%
  Segregation of duties	73 months	None	0%

In the above example, if you select the "Manage Skills and Competences" 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.

5. Click **OK**.
The list of controls to be assessed in a particular context appears.
6. Enter the control **Design** and **Effectiveness** quality level:
 - Pass
 - Fail
7. After answering questions, click **OK**.

Assessments are created in the **Assessment** page of the control properties. For more details, see [Displaying the Results of Control Assessment](#).

ASSESSMENT CONTROL RESULTS

Displaying the Results of Control Assessment

To display the results of assessments performed on a control:

1. From the control register, 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** is automatically calculated from the specified characteristic values (Pass/Fail).

Approval of needs control

Assessment

To assess the object directly, click on the button "Perform Assessment". All past assessments are displayed in the list below. To filter assessments by context element & assessment method, select the relevant context element(s) and corresponding template(s). If nothing is selected in the 'Context Element' AND 'Assessment Template' fields, ALL assessments are displayed. Only contexts that have been previously assessed are available. All assessments (performed directly or through assessment sessions) are displayed.

Context Element(s) Assessment Template Apply Filters

Perform Assessment

<input type="checkbox"/>	Date	Assessor	Organiza...	Org-Unit	Design	Effectiveness	Control Level
<input type="checkbox"/>	4/16/2...	Christophe	Needs	Italy,Subsi...	✓ Pass	✓ Pass	✓ Pass

See also: [Assessment Result Computing Mode](#).

The IRM functional administrator only can delete assessment results (that is to say assessment nodes).

To delete an assessment node, select it and click **Delete**.

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.

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 [Control Assessment Follow-Up Reports](#).

Assessment Result Computing Mode

Metaattribute	Computed / Not Computed	Explanations
Control Design (IC)	Computed through the [Internal Control - Control Attributes] macro	- 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	- 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)



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.

The number of checklists sent depends on the total population size and sample size.

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

- ✓ [Preparing Control Execution](#)
- ✓ [Continuous Control Assessment Template](#)
- ✓ [Creating Execution Campaigns](#)
- ✓ [How an Execution Campaign Works](#)
- ✓ [Completing Control Execution Check-Lists](#)
- ✓ [Managing Execution Check-Lists](#)
- ✓ [Check-List Results](#)
- ✓ [Control Execution Reports](#)

PREPARING CONTROL EXECUTION

To be able to launch execution campaigns, you must first define the necessary conditions for control execution:


- questions
- steering calendars
- total population and sample size
- respondents
- control contextualization

Defining Questions on Controls

You must define the content of check-lists used at control execution.

The questions to be defined on controls are called “control steps”.

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 [Managing Questionnaire Templates](#).

Defining Steering Calendars on Controls

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


 You can specify the control execution steering calendar only after having created the questionnaire (that is to say control steps).

To create a steering calendar, see [Managing Steering Calendars](#).

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.
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

Modifying a steering calendar after campaign creation

If you modify the steering calendar on controls included in a campaign in progress, you need to re-schedule check-lists.

To ensure all check-lists are properly scheduled:

1. In the properties of an execution campaign, select the **Sessions** page.
2. Click the **Schedule Checklists** button.

☛ This applies to controls that use a steering calendar not included originally in the campaign, or controls whose steering calendar has been modified.

Defining the Total Population and Sample Size

☛ This step is optional.

You can define:

- the **Total Population Size**: total number of objects
- The **Sample Size**: percentage of population that is actually controlled

☛ This information is optional.

For example:

- **Control**: "Check the contract signature"
- **Total population**: 20 (20 contracts)
- **Sample size**: 10% (2 controls are checked)

The control owner receives a check-list with two lines to fill in (one line per contract)

To specify the total population and sample size:

1. In the control properties, select the **Execution** page.
2. Expand the **Execution Method** section.

3. Specify the following information:

^ Execution Method

Execution Frequency	Method	Steering Calendar
Monthly	By Sample	Internal Control - Monthly Execution
Total Population Size	Sample Size	Compliance Rate Threshold
20	10%	80%

☛ The **Compliance threshold** enables to compute the execution result.
The control is "Passed" if the compliance rate is greater than or equal to the compliance threshold.

Defining Respondents

Check-list respondents are control owners for a specific entity.

On each control you must define persons responsible for completing execution check-lists.

The logics behind respondent definition is the same as for control assessment by entities. See [Control Assessment by Entity](#).

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](#).

CONTINUOUS CONTROL ASSESSMENT TEMPLATE

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

The "Continuous Control" execution 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.

Respondents

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

Check-lists sent

A check-list is sent for every assessed control/respondent node.

If the respondent is in charge of several controls, he receives several questionnaires.

The number of assessment nodes of a check-list depends on the total population and sample size specified in the control properties.

For example:

If total population size = 10 and if sample size = 20%

Then the number of assessment nodes = $10 \times 0.2 = 2$

☛ For more information, see [Defining the Total Population and Sample Size](#).

Answer computation

Only OK/KO type of answers are taken into account.

☛ For more information on how to define questionnaire answers, see [Summary of Question Types](#).

Aggregated results

All nodes with the same control and context are aggregated. The following values are calculated:


- **Compliance rate**: number of "Pass" nodes / total number of nodes
- **Completion rate**: percentage of questionnaires that are totally completed
- The **Execution rate** is considered "Pass" if the compliance rate is greater than or equal to the compliance threshold.

☛ The compliance threshold has been specified in the properties of the assessed control.

CREATING EXECUTION CAMPAIGNS

To create an execution campaign:


1. In the navigation menu, select **Execution > Campaigns**.
2. Click **New**.

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


You are now going to define the way of specifying your campaign scope.

3. In the field **Define scope via a tree**, select:

- **Yes**: a tree enables to define the scope in a very precise way, but it does not allow to take into account the controls added after campaign creation.

 If you choose this option, see [Defining scope via a tree](#).

- **No**: a **Root entity** field is displayed.

 The scope is recreated each time a session is launched. This means that if new controls have been added, they are taken into account at the next planned execution session.

4. Modify the dates suggested if needed.

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

5. Click **Next**.

The campaign summary appears.

 See [Displaying the Execution Campaign Summary](#).

6. Click **OK**.

The campaign appears in the list. It is started automatically:

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

 See [Consulting Execution Campaign Schedule](#).

Defining scope via a tree

To define the campaign scope:

1. See [Creating Execution Campaigns](#).
2. Display the wizard that enables to define the scope.

3. Select all the controls to be assessed from the tree.
Some columns help you choose the controls to be selected:

- **Compliance rate**



The compliance rate is the percentage of "Pass" controls.

- **Open Issues** (number)

Campaign Scope

i

 Please select all Controls to be assessed

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

-

+

	Compliance Rate	Open Issues
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input checked="" type="checkbox"/> </div> <div>World@Hand Corporation</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input type="checkbox"/> </div> <div>Corporate Headquarter</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input checked="" type="checkbox"/> </div> <div>Regional Headquarter</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input type="checkbox"/> </div> <div>Car Rental Department</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input checked="" type="checkbox"/> </div> <div>HR Department</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input checked="" type="checkbox"/> </div> <div>Develop and Manage Human Capital</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input type="checkbox"/> </div> <div>Manage HR Administration and Pay...</div> </div> <div style="margin-left: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <input checked="" type="checkbox"/> </div> <div>Manage Skills and Competences</div> </div> </div> </div> </div> </div> </div> </div> </div>		

☒

Control on special orders

0%

2

☐

Segregation of duties

0%

0

Displaying the Execution Campaign Summary

After selecting the campaign scope (via a root entity or a tree), the summary of the campaign is displayed. It contains the following:

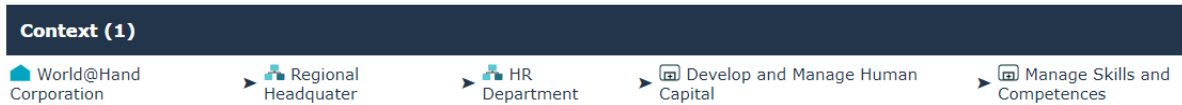
General information (Overview)

Number of:

- **errors::** errors prevent from launching the execution campaign:
 - the respondent is not specified
 - the steering calendar is not specified
- **Warnings,** for example:
 - the total population or sample size is not specified
 - the respondent e-mail is not specified
- assessed objects
- assessment contexts
- respondents

Contexts

Contexts appear in the form of a process and entity hierarchy



Respondents

Respondents execute controls.

🔍 For more details on control responsibilities, see [Responsibilities concerning Controls](#).

🔍 If no respondent has been specified, right-click the control and enter it in the **Responsibilities** section.

Assessed objects

Assessed controls are classified by execution frequency, showing in columns:

- the respondent
- contexts: entities and organizational/business processes
- total population size
- sample size
- compliance rate
- number of open issues

HOW AN EXECUTION CAMPAIGN WORKS

Control Execution Periodicity

An execution campaign groups several execution sessions.

An execution session groups a set of controls to be executed on the same date.

Execution 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 others controls

Controls are therefore grouped in each session according to the steering calendar to which they have been connected. See [Defining Steering Calendars on Controls](#).

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

Examples of Session Automatic Launch

Execution sessions are launched according to the following information:

- begin and end dates of the execution campaign
- begin/end dates and recurrences specified on the steering calendar of the controls

➡ For more details on steering calendars, see [Defining Steering Calendars on Controls](#).

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.

Consulting Execution Campaign Schedule

To consult dates of the next execution of a campaign in progress:

1. In the navigation menu, select **Execution > Campaigns**.
2. Open the properties of the execution campaign and select the **Gantt** page.

The list of timespots defined by the steering calendar appears.

To display the properties of the execution session from the Gantt chart:

1. Right-click the execution session and select **Properties**.

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.

Defining Reminders

The execution campaign manager can define reminders, which consists in sending respondents e-mails after sending and/or before closing of the check-list.


Modifying reminders provided as standard

Some reminders are provided as standard. You may modify the values specified.

To modify the reminders provided as standard:

1. In the navigation menu, select **Execution > Campaigns**.
2. Open the properties of the execution campaign.
3. In the **Characteristics** page, expand the **Check-list Reminders and Early Closure Dates** section.

4. For each steering calendar specify the following:
 - Number of **Days after check-list submission**
 - Number of **Days before check-list closure**

 Every change in the reminder definition will be taken into account when the next execution session is launched.

Deactivating reminders

To deactivate reminders:

1. Empty the cells of the reminder definition table.

Closing Check-lists

You can choose to close check-lists of an execution campaign connected to a specific steering calendar.

This enables to avoid leaving check-lists open for too long (if campaigns are launched infrequently for example).

To do this:

1. In the navigation menu, select **Execution > Campaigns**.
2. Open the properties of the execution campaign.
3. In the **Characteristics** page, expand the **Check-list Reminders and Early Closure Dates** section.
4. In the row corresponding to the steering calendar, specify a value in the **Close after (days)**.

If you specify 60 in this column, check-lists will be closed 60 days after the start of the execution session.

COMPLETING CONTROL EXECUTION CHECK-LISTS

When the execution campaign has started, you can complete check-lists. To do this, you may login with the "IRM Contributor" profile.

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

Accessing Execution Check-Lists

To access execution check-lists:

1. Click the link in the e-mail that you received:

☛ (variant 1) In the home page of the "IRM Contributor" desktop, click **My Tasks > Execution Check-Lists**.

☛ (variant 2) In the **HOPEX IRM** desktop, select **My Tasks > Execution > Check-lists To Complete**.

Completing a Check-List

To complete the check-lists addressed to you:

1. See [Accessing Execution Check-Lists](#).
2. Click the name of the check-list to open it.
3. Answer the questions in the table that appears.

☛ If the control has already been executed in this very same context, answers given in the last check-list are displayed by default.

4. Click **Submit** and **Complete**.

☛ You can click **Save for later** if you want to submit your answers later on.

Transferring a Check-List

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. See [Accessing Execution Check-Lists](#).
2. Click the name of the check-list.
3. Click **Submit** then **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.

MANAGING EXECUTION CHECK-LISTS

Accessing Check-Lists


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

To access check-lists:

1. 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


Reassigning Check-Lists

If a transfer request has been addressed to you, you must reassign the check-list to another user.

 For more details on how to transfer a check-list, see [Transferring a Check-List](#).

To reassign a check-list:

1. In the **HOPEX IRM** desktop, select **My Tasks > Execution > Check-lists To Reassign**
2. Select a check-list and open its properties.

 For details, see [Reassigning questionnaires](#). The principle is the same as for assessment questionnaires.



CHECK-LIST RESULTS

To display the results of execution check-lists:

3. In the control properties, select the **Execution** page.
4. Expand the **Continuous Control Results** section.

Assessment nodes (controls executed in a specific context) are displayed as a table.

Results are displayed in columns:

- **Completion rate**: percentage of check-lists that are entirely completed (out of all check-lists)
- **Compliance rate**: number of "Pass" nodes / total number of nodes
 *Only questions of OK/KO/NA type are used for compliance rate computation.*
- The **Execution rate** is considered "Pass" if the compliance rate is greater than or equal to the compliance threshold.
 ***Sample size** and **Compliance threshold** are reminded for your information. Corresponding values were specified in the control properties.*

CONTROL EXECUTION REPORTS

Reports allow you to follow up check-list progress and results.

To access control execution reports:

- 1 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)

🔍 This report is available only in the **Analysis** navigation tab.

Consolidated Execution Results

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

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

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 OK instances** (number of instances considered as satisfactory ("pass"))
 - a **% of OK instances** (considered as satisfactory ("pass"))

Following Up Execution Sessions

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

Access path

Analysis > Controls > 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



MANAGING COMPLIANCE



HOPEX IRM 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)
 - ☛ *To be able to use the import wizard, you need to have **HOPEX UCF**.*
- define regulations with which the organization must comply, as well as its internal business policies
- define the perimeter of entities and processes subject to compliance
- assess IT compliance to applicable regulations
 - ☛ *An specific assessment template is available. See [Control Assessment by Entity and Regulatory Framework](#).*
- generate regulatory and IT compliance reports.

- ✓ [About Unified Compliance Framework](#)
- ✓ [Managing the Regulatory Environment](#)
- ✓ [Managing the Compliance Register](#)
- ✓ [IT Regulatory Compliance Reports](#)

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®](#).

When you use UCF, the whole compliance project becomes less expensive than if chose to deal with each regulation separately.

Main UCF Concepts

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	① 00763				
▼ Privacy protection for information and data	① 00008				
> Establish and maintain a privacy framework that protects restricted data.	② 11850				
▼ Establish and maintain a Customer Information Management program.	② 00084				
> Establish and maintain a customer due diligence program, as necessary.	① 13618				
Define and assign the data controller's data quality roles and responsibilities.	① 00085				
> Establish and maintain customer data authentication procedures.	① 13187				
Check that personal data is complete.	① 00090				
Keep personal data up-to-date and valid.	① 00091				
Maintain personal data in a form that does not permit the identification of dat...	① 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 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 Common Control	Control directive	

MANAGING THE REGULATORY ENVIRONMENT

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 regulatory environment in **HOPEX**:

- 1 In the navigation menu, select **Environment > Compliance**.

Using UCF Import

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 relevant data from the UCF Common Controls Hub (Authority Documents, Citations and Controls)
- declaring the appropriate articles as relevant for your organization: see [Defining the Applicable Regulatory Content](#).

To import UCF data:

1. In the navigation menu, select **Environment > Compliance > Regulatory Frameworks**.
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?	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**.


Defining the Applicable Regulatory Content

Regulatory content relevance

All the articles/sections of an imported regulatory framework are not applicable to your organization.

Compliance officers can inspect the imported regulatory frameworks and specify which ones are applicable.

Only the applicable articles and sections will appear in **HOPEX** registers for your stakeholders.

 The regulatory content you directly create in **HOPEX** is automatically considered as compliant (applicable).

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.
- specify the content applicable to your organization

Selecting relevant content for your organization

To declare regulatory content as relevant:

1. From the navigation menu, select **Environment > Compliance > Control Directives**.
2. Expand the tree if necessary and select the check-box corresponding to the regulatory frameworks/articles/sections you must comply with.

	Applicable	Regulatory Children
 CobiT	<input type="checkbox"/>	40
  AC1 Source Data Preparation and Authorisation. Ensure ...	<input checked="" type="checkbox"/>	0
  AC2 Source Data Collection and Entry. Establish that dat...	<input checked="" type="checkbox"/>	0
  AC3 Accuracy, Completeness and Authenticity Checks. E...	<input checked="" type="checkbox"/>	0
  AC4 Processing Integrity and Validity. Maintain the integ...	<input checked="" type="checkbox"/>	0
  AC5 Output Review, Reconciliation and Error Handling. E...	<input type="checkbox"/>	0
  AC6 Transaction Authentication and Integrity. Before pa...	<input type="checkbox"/>	0
  PO1. Define a Strategic IT Plan	<input type="checkbox"/>	1

 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 register. See [Managing the Compliance Register](#).

MANAGING THE COMPLIANCE REGISTER

In the compliance register, internal controllers can manage:

- regulations: regulatory frameworks, articles and control directives applicable to the organization.

☛ If you have regulation frameworks and requirements in your repository and if you want to be able to reuse them in **HOPEX IRM**, see [Reusing Regulation Data](#).

☛ The compliance register does not display everything that has been imported from UCF. It only displays the regulation articles the compliance officer has declared as applicable after import. For more details, see [Defining the Applicable Regulatory Content](#).

- rules that are internal to the organization: business policies

Concepts Used in the Compliance Register

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.
Article (of regulatory framework)	An article is a citation from a regulatory framework and is usually associated to a mandated control directive.
Section (of regulatory framework)	A section is a citation from a regulatory framework without any mandated control directive, but containing other sections or articles.
Control directive	Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.
Policy framework	A policy framework consists of a number of business policies. Policy frameworks may contain sections.
Business policy	A business policy is an internal document issued by an organization (security measure, best practice, etc.).

Accessing the Elements of the Compliance Register

You can view the elements of the compliance register via different lists and trees.

Displaying elements as a list

Your control directives and business policies can be classified in different lists available from a drop-down menu:

- All control directives / business policies
- Control directives/business policies without controls
- Control directives/business policies with controls never executed
- Control directives/business policies with deficient controls

To access these lists:

- 】 In the navigation menu, select **Registers > Compliance**.
 - **All control directives**
 - **All business policies**

Columns indicate, for each control directive:

- whether the control directive/business policy constrains your organization
- the number of implementing controls

To list existing implementing controls or create one:

- 】 Open the properties of a control directive/business policy and use the **Enforcement** section.

Displaying control directives in a tree of regulatory frameworks

To display control directives in a tree:

- 】 From the navigation menu, select **Registers > Compliance > By Regulatory Framework**.

This tree enables you to view articles and control directives your organization needs to comply with. It displays:

- regulatory frameworks
- control directives implementing articles
- associated controls

Displaying business policies in a tree

To display control directives in a tree:

- 】 In the navigation menu, select **Registers > Compliance > By Policy Framework**.

This tree enables you to view business policies your organization needs to comply with.

It displays:

- the number of implementing controls
- compliance rate



The compliance rate is the percentage of "Pass" controls.

- the control level



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

Viewing Regulatory Frameworks

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

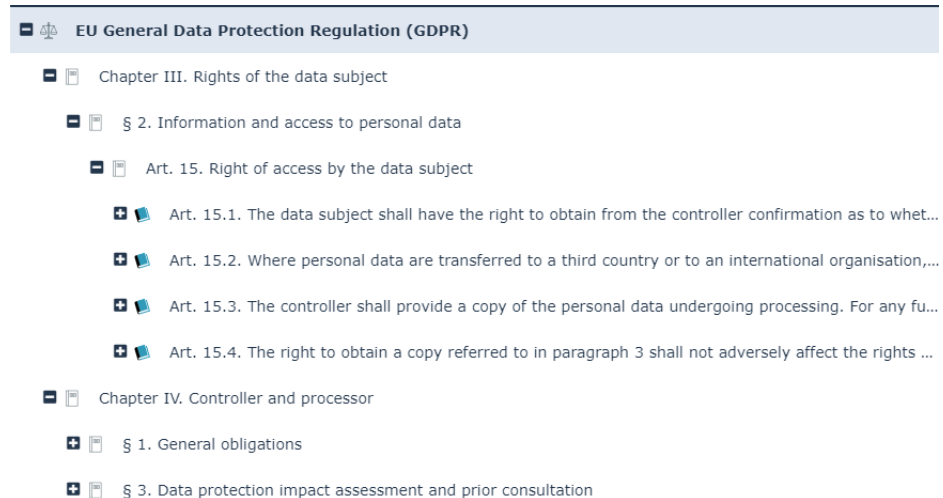
☛ *Regulatory frameworks correspond to UCF imported Authority Documents.*

Accessing regulatory frameworks

A regulatory framework tree displays relevant regulation articles.

To access the regulation framework tree:

- 1 From the navigation menu, select **Registers > Compliance > By Regulatory Framework**.



☛ *The regulation articles displayed are those that were declared as relevant in **Environment > Compliance > Control Directives**.*

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](#).*
- **HOPEX** implementing controls, if any.
☛ *For more details on controls, see [Managing Controls](#).*

Regulatory framework overview & description

The **Overview** section of the regulatory framework characteristics enables you to display general characteristics originating from the Common Controls Hub.

✎ These characteristics cannot be modified if the content comes from UCF.

Description

URL

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv: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.

Content of a regulatory framework

To access the relevant regulatory content of a regulatory framework:

1. From the navigation menu, select **Registers > Compliance > 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**

Regulation Articles

Regulation Articles List

Hierarchy by Sections

EU General Data Protection Regulation (GDPR)

Chapter II. Principles

Art. 5. Principles relating to processing of personal data

Art. 6. Lawfulness of processing

Art. 7. Conditions for consent

Viewing Regulation Articles

An article is a citation from a regulatory framework and is usually associated to a mandated control directive.

☛ *Regulation articles correspond to the imported UCF Citations. For more details, see [Main UCF Concepts](#).*

☛ *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



Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

- implementing controls, if any



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

Accessing regulation articles

To access regulation articles:

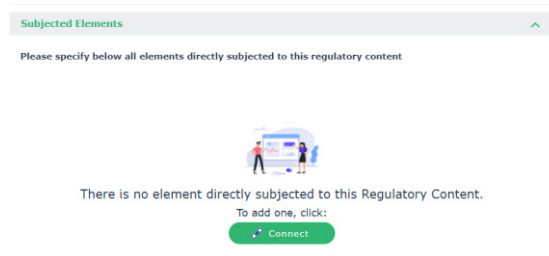
- 】 From the navigation menu, select **Registers > Compliance > By Regulatory Framework** and expand the tree.

Connecting or viewing 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:

- 1 In the property page of the 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.

You can also view objects that are indirectly linked to the regulation article.

Example of indirect link: If a regulatory framework is linked to an entity, the entity is indirectly linked to all the regulation articles and sections of the regulatory framework.

Enforcement of a regulatory article

To know more about the enforcement of a regulation article:

- 1 Open the property pages of the regulation article and expand the **Enforcement** section.

You can view:

- Its associated **Control Directives**
 - ☛ You can view the qualification of the control directive in the corresponding column:
 - mandated
 - implied
 - implementation
- its **Implementing Controls**

Implementation controls that appear in this list are those connected to control directives of this section.

 - ☛ 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 are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.

☛ *Control directives correspond to Common Controls imported from UCF. For more details, see [Main UCF Concepts](#).*

Accessing control directives

To access the control directives of your register:

- 1 From the navigation menu, select **Registers > Compliance > All Mandated Control Directives**.

☛ *First-level Implied control directives appear in this list only if one of their children is mandated.*

Some columns indicate:

- whether the control directive constrains the organization
- the number of implementing controls associated

From the drop-down list you can view the control directives sorted according to different criteria:

- **Control directives without controls**

☛ *To create a control on a control directive, expand the **Implementation** section.*

- **Control directives with controls never executed**
- **Control directives with deficient controls**

Viewing articles associated to a control directive

A mandated control directive is associated to a regulation article.

It is beneficial to have several regulation articles in the **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

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 displayed in a tree that enables to view their inter-relations.

All Control Directives are presented below in a tree structured around the Control Directives supporting one another, as originally defined in the UCF Common Control Framework.

Enforcement Level for each is derived from Control Directives mandated against a Regulation Article. Any Control Directive supported by a Mandated Control Directive is "implied" while the Control Directives supporting the same Mandated Control Directive are "Implementation".

Any "Implied" Control Directive will contain a Mandated Control Directive in its hierarchy. Any "Implementation" Control Directive will appear under a Mandated Control Directive.

You can focus on one root Control Directive of your Control Framework at a time by selecting it from the filter box.

Filter By:

Supported directive

Directive

Supporting directives

Establish and maintain a Customer Information Management program.

Characteristics

Name
Establish and maintain a Customer Information Management program.

Control Nature
Preventive

Enforcement Level
Implied Control

External Identifier(s)
84

Regulation Articles

Directives

Supporting Directive Supported Directive

Name **Enforcement Level**

Privacy protection for information and data Mandated Control

Having several control directives in the **Supported Directive** tab of a 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 on a control directive:

1. From the navigation menu, select **Registers > Compliance > All Mandated Control Directives**.
2. Open the properties of a control directive.
3. Expand the **Implementation** section.



You can also create controls from this section.

You are given information on the control as well as on its execution results:

- **Control nature**
 See [Control nature](#).
- **Control level**
 The Control level characterizes the efficiency level of control elements deployed (controls) to mitigate the risk.
 See [Control level](#).
- **Latest compliance rate**
- **Latest execution result**
 For more details on control contextualization see [Executing controls](#).

Attaching business documents or external references

You may attach business documents to a control directive or create an external reference of URL type.

IT REGULATORY COMPLIANCE REPORTS

HOPEX IRM provides reports that enable to follow the IT and regulatory compliance process.

Reports enable to:

- view the compliance level of an entity with regulations.
➤ See [Regulatory Compliance by Entity](#).
- distinguish, for each regulatory framework, between control directives implemented by controls and control directives not implemented by any controls.
➤ See [Regulatory Framework Implementation](#).
- view compliance level for each regulatory framework.
➤ See [Compliance by Regulatory Framework](#).
- follow compliance process progress.
➤ See [Regulatory Compliance Overview](#).
➤ See [Regulatory Compliance Progress](#).
- view issues that impact a given control type (a control type related to IT compliance for example)
➤ See ["Issues by Impact" Report](#).

Regulatory Compliance by Entity

The "Regulatory Compliance by Entity" report displays the aggregated entity compliance level to applicable regulatory frameworks.

This report displays a tree of all the entity processes and applications for which a control connected to regulations has been assessed.

Access path

Analysis > Compliance > Regulatory Compliance by Entity

Parameters and Launch

To launch the report "Regulatory Compliance by Entity":

1. Enter the required parameters.

Parameters	Remarks
Entity	Mandatory Entity whose compliance level is to be computed.
Begin and end date	Optional Enables to define the time interval to take into account to aggregate assessment results. If no date is specified, all assessment data is taken into account for compliance level computation.

2. Click **Launch Aggregation**.

Parameters

Name
My report - Regulatory Compliance by Entity

Entity*
Adobe Systems

Begin Date

End Date

Generate Aggregation

3. Click **OK**.

Example

	Compliance Level
Administration department	4%
GDPR	4%
Process personal data relating to criminal offenses when required by law.	0%
Approval of needs control	0%
Needs	Not Assessed
Include the organizational structure and contact information in the Binding Corporate Rules.	0%
Sensitive outbound Application Communications are cyphered	0%
Billing	Not Assessed
Allow individuals to change their personal data collection consent preferences.	100%
Control all methods of remote access and teleworking	100%
Booking Management	Pass

Results for each object in this report are computed as follows:

Object type	Calculation
Application/Process (in the control scope)	Last control assessment in the context of the application or process. Possible results: - Pass - Fail - Not assessed
Control (implementing a control directive)	Percentage of pass controls (for context applications or processes) Note: here, Not assessed = Fail
Control directive (of a regulatory framework)	Average of control levels for controls connected to a control directive
Regulatory framework (with the root entity of the tree in its scope)	Average of control levels for control directives connected to the regulatory framework
Entity	Average of control levels for regulatory frameworks connected to the entity.

Regulatory Framework Implementation

This report enables the compliance officer to make sure control directives are appropriately implemented by controls.

It consists in a stacked bar chart, which shows the overall coverage of a given list of regulatory frameworks. A regulatory framework is considered as implemented if all the control directives are connected to a control.

Access path

Analysis> Compliance > Regulatory Framework Implementation

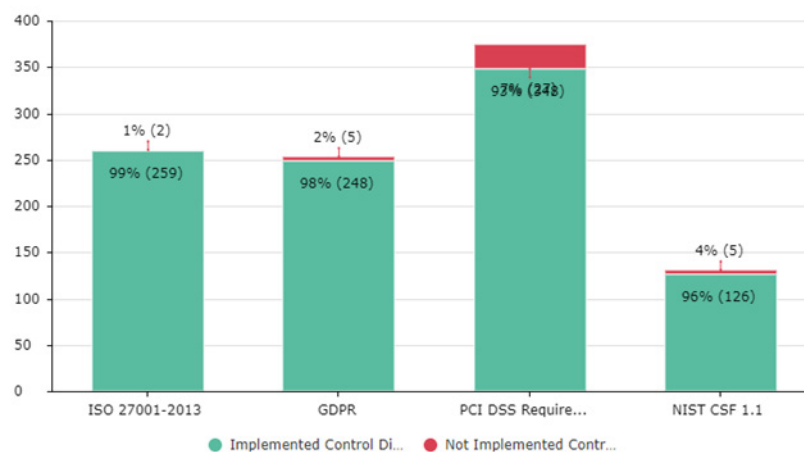
Parameters

Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frameworks.

Results

The report distinguishes, for each regulatory framework, the percentage of:

- control directives connected to at least one control (**implemented control directives**)
- control directives not connected to any control (**Not implemented control directives**)



Compliance by Regulatory Framework

☛ This report is also available in the form of widget to be added to your dashboard. To add it, from the navigation menu, click **Dashboard** then **Add a widget > IRM > Compliance**.

It consists in a stacked bar chart, which shows the level of compliance with a list of regulatory frameworks.

Access path

Analysis > Compliance > Compliance by Regulatory Framework

Parameters

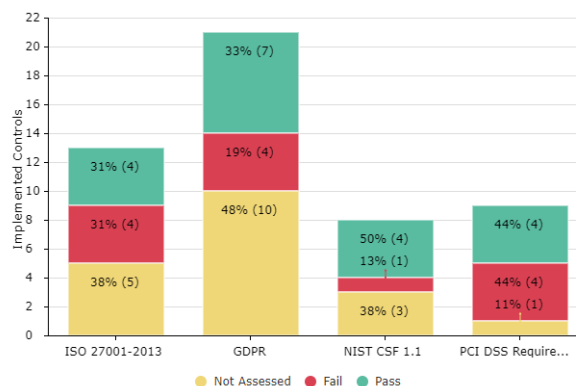
Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frameworks.

Results

Results are displayed in the form of bar charts.

Each bar displays the number of controls associated to control directives and enables to classify them as follows:

- **Pass**: controls whose Control Level = 100% (successfully passed the assessment)
- **Fail**: controls whose Control Level < 100% (did not obtain a satisfactory score)
- **Not assessed**: controls with no control level



Regulatory Compliance Overview

The "Regulatory Compliance Overview" report enables to follow-up the details of compliance to a specific regulatory framework.

Access path

Analysis > Compliance > Regulatory Compliance Overview

Parameters

Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frameworks.

Results

From this report you can monitor, for each regulatory framework:

- **Compliance %**: percentage of pass controls out of the number of controls connected to the regulatory framework control directives.
- **Implementation %**: percentage of assessed controls out of the number of controls connected to the regulatory framework control directives.
- control assessments
 - **Control Level**
 - **Last assessment control**
- issues and action plans implemented:
 - **issue**
 - **% of action plan progress**
 - **action plan status** (on time, delayed)
 - **action plan cost** (estimate of the action plan cost)

Implementing Control Control Level Action Plan Status

Regulatory Framework	Effective Date	Control Directive	Implementing Control	Control Level	Last Assessment	Issue	Action Plan	Action Plan Completion
EU General Data Protection Regulation (GDPR)	4/27/2016	Control Directive MII	Control-1	Not Assessed				0.0%
		Collect and record personal data for specific, explicit, and legitimate purposes.	Collect and record personal data for specific, explicit, and legitimate purposes.	Fail	2/8/2021			0.0%
		Establish, implement, and maintain a personal data transparency program.	Establish, implement, and maintain a personal data transparency program.	Fail	2/8/2021			0.0%
		Obtain explicit consent directly from the data subject prior to the use of that person's sensitive data.	Obtain explicit consent directly from the data subject prior to the use of that person's sensitive data.	Fail	2/8/2021			0.0%
		Collect the minimum amount of personal data necessary.	Collect the minimum amount of personal data necessary.	Pass	2/8/2021			0.0%
		Update the privacy policy, as necessary.	Update the privacy policy, as necessary.	Pass	2/8/2021			0.0%
		Process personal data lawfully and carefully.	Process personal data lawfully and carefully.	Fail	2/8/2021			0.0%

Regulatory Compliance Progress

This report is a radar chart showing the evolution over time of the compliance level of one entity with a given set of regulations.

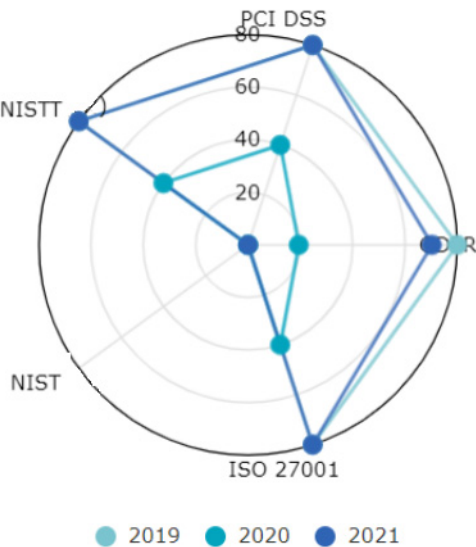
Access path

Analysis > Compliance > Regulatory Compliance Progress

Parameters

Parameters	Remarks
Entity	Organization whose compliance level is to be computed
Regulatory framework	Regulations to include in the chart
Calendars	Time periods taken into account to follow-up the evolution of the compliance level over time

Report example



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 IRM** allows internal controllers to:

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

The testing process consists of three phases:

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

PREPARING CONTROL TESTING

➤ See also [Contextualizing Controls](#).

➤ See also: [IRM Functional Administration](#).

Defining Test Sheet Questions

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

To create testing steps on a control:

1. In the control properties, select the **Testing** page.
2. In the **Test Steps** section, click **Create a Questionnaire Template**.
3. In the dialog box that appears, drag & drop a DropDown question.
4. Enter for example the following values "OK/NO/NA".
5. Click **Save and Close**.

Defining Testing Methods

➤ *To be able to define the testing method, you need to have created questions (testing steps) on controls.*

To specify control test characteristics:

1. In the control properties, select the **Testing** tab.
The **Testing Method** section presents characteristics concerning testing.
2. Specify the **Testing Frequency**:
 - Yearly
 - Quarterly
 - Half-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](#).*

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:

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

Creating Test Plans

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 > Test Plans**.
2. Click the **New** button.
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 only have **HOPEX Internal Control**, 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 IRM Manager.



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

Creating a test

To create a test:

1. Click **Test > Test Plans**.
2. Open the properties of the plan that will include the test to be created.
3. Select the **Tests** 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:

1. Click **Test > Test Plans** and expand a plan.
The tests (or audits, depending on the plan nature selected) corresponding to the plan appear.

Defining test properties

You can specify certain information on tests.

See also [Viewing a test dashboard](#).

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:

- **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 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**
- **Justification** of the test

Line

In this section 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 this 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 this section you can specify the stakeholders of a test:

- **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

In this section you can specify the 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 the **Conclusion** section, you can specify:

- **Key Strengths**
- **Key Weaknesses**
- **Evaluation**: good overall level, can be improved, etc.

 The value specified here is displayed in the test dashboard, at the top of the **Characteristics** page.

Test Activities

A specific page in the properties of the test enables to view test activities.

Deficiencies

A specific page in the properties of the test enables to view deficiencies.

Viewing a test dashboard

To access a test dashboard:

1. See [Accessing tests](#).
2. Open the properties of a test.

The **Characteristics** page displays a dashboard containing essential information about the test:

- **Progress** % = number of test activities in "closed" status / number of activities in the test
- **Evaluation** of the test:
 - Good overall level
 - Can be improved
 - etc.

 This evaluation is performed by the audit director.

- **Issues**: displays the number of issues

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 > Test Plans**.
The list of plans appears.
2. Click the icon of the plan in question and select **To Be Validated > Set As Template**.

Selecting tests to be executed

Viewing the test coverage report

HOPEX IRM 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. (Optional) select the score obtained by the test or its status.

For each tested entity the report presents:

- the **Number of tests** executed between the two dates (effective begin and end dates)
- the **End date** of the last test (effective end date), or its state if it is still in progress
- the name of the **Last Test**.
- the **Score** of the last test.

To generate tests corresponding to one or several entities:

1. 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.

Viewing previous audit expenses

A report allows you to view expenses of previous audits.

To access this report:

1. Click **Test > Test Plans**.
2. Select a plan and in its properties select the **Reports** page.
3. In the drop-down list, select **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 IRM 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 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 IRM Manager) to plan the different tests of a test plan.

To display this report:

1. Under **Test** > **Test Plans**, select the plan properties.
2. Select the **Schedule** page.

A Gantt chart describes tests of the plan.

The schedule shows data of the current year. You can view tests within the framework of a more specific time period.

To define the display period in the Gantt chart:

- select a calendar period, or
- specific begin and end dates.

To modify dates for an test in the chart:

1. Click the center of the period and move the mouse to simultaneously move the begin and end dates.

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. Select the **Assign Resources** page.

 *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, 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
 - Yellow 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 top right frame, select a person and select the **Assign** check box.

 To remove an assignment, perform the same procedure and clear the **Assign** check box.

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 step in the workflow that consists in publishing the test.

Creating notification letters

To create the test notification letter:

1. 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:

1. Open properties of the test.
2. Select the **Documents** page and the **Business Documents** tab.

3. Drag and drop the notification letter that was previously generated. The document appears in the list of documents attached to the test.
4. Open the document properties and in the **Document Pattern** field, select "Notification Letter".

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 IRM 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 IRM 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.

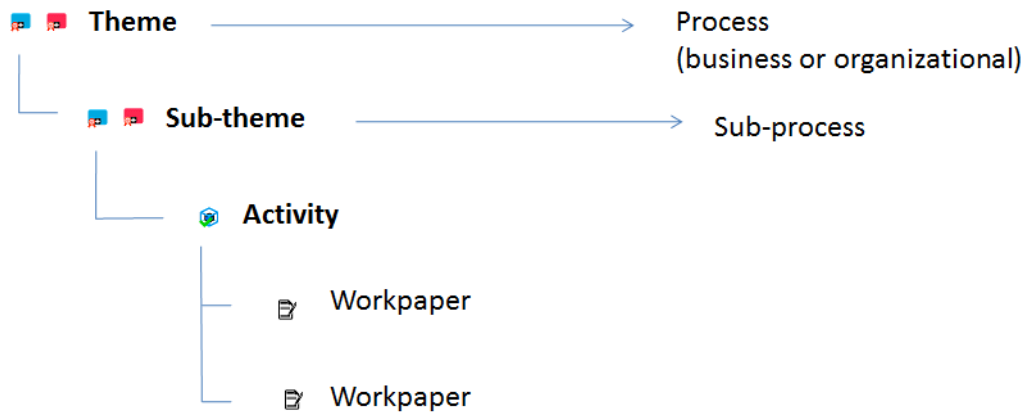
A workpaper is generated for each generated test activity. For more details, see [Creating workpapers](#).

Creating work programs automatically

To create a work program automatically:

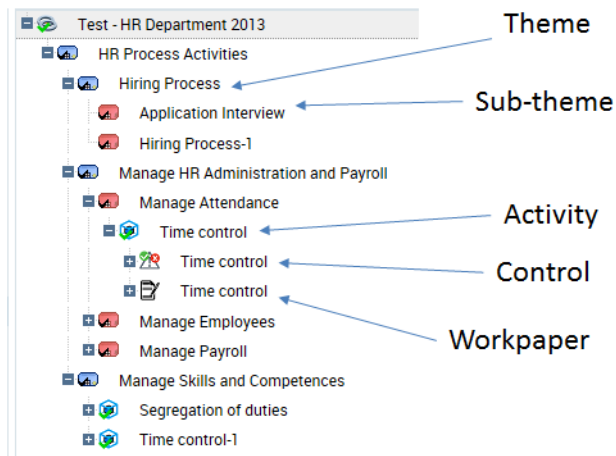
- 1 Click the test icon and select **Generate Work Program**.
This is going to duplicate the process tree for the entity within the test scope.

If processes are explicitly specified in the test scope, only these processes are 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** page 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. Connect the activity to a **Theme** if you want the activity to be located under a theme in the tree.
5. Connect the test activity to a control.
6. Select the **Owner** of the test activity, who can be a controller or the lead controller of the current test.
7. Indicate the **Estimated Workload**.
 *You can later manually enter the effective workload on this activity.*
8. Click **OK**.

Assigning activities

Assigning an activity

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 **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.

Assigning multiple activities to the same controller

To assign multiple activities to the same controller:

1. In the properties of the test, select the **Activities** page.
2. Select your activities and click the **Assignment** button.
3. In the multiple assignment wizard, select the **Test Activity Owner**.

4. Click **OK**.

Reviewing the Work Program

The lead auditor can proceed with a report on the work program. This report allows to 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:

- 1 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:

- 1 In the **Work program** page of the test, 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 modify the work program in Excel.

When the work program has been modified, you must create a business document in **HOPEX IRM** 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. Select the **Business Document** tab and drag-and-drop the work program Excel document.

The modified work program is now stored in the **HOPEX** repository.

 In the properties of the business document, you can specify "Work Program" as a **Document pattern**.

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:

1. Click the icon of the test and select **To Be Validated** > **Validate**.

Executing administrative tasks

Planning resources

Controllers can be assigned different tests at the same time. It is therefore important to enter the time allocated for each auditor to a test.

To indicate for each controller the time to be allocated to a test:

1. In the properties of the test, expand the **Responsibilities** section.
2. Select the **Controller in test** tab.
3. 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 internal controller needs to consult his/her work program.

To access tasks to perform:

- 】 From the navigation menu, select **My Tasks > Test > Activities to Perform**.

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.

Assessing test activities

Having specified test sheets, the controller can globally assess the test activity.


 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:

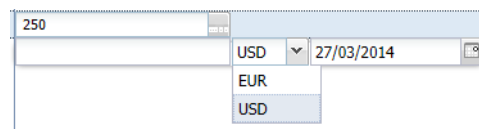
1. In the **HOPEX IRM** navigation menu, select **My tasks > Time & Expenses > Expenses**.
2. Click **New**.
3. In the **Expense Owner** field, select the audit/test concerned.

 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 '250'. To its right is a dropdown menu currently displaying 'USD'. Below the dropdown, the options 'EUR' and 'USD' are visible. 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 > Time & Expenses > 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 > Time & Expenses > TimeSheets**.
The time sheet displays one line per audit.
2. Enter for each day the number of hours spent on each audit.
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 however 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.

In the properties of an issue you can qualify its **Impact**.

Saving test evidence

You can connect business documents or specify an URL address 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. In the **Business Document** drag-and-drop a document.



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.

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:

1. 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 for 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:

- 1. 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:

- 1. 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:

- 1. In the properties of a test, select the **Reports > Assessment** page.

Several reports are proposed:

- Controls (Failed, Passed, Not evaluated)
- Action plan breakdown by priority (low, medium, high)
- Summary table of above elements
- Issues by theme

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:

- 1. In the navigation menu, select **My Tasks > Remediation > 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:

- 1. 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:

1. 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:

1. In the **HOPEX IRM** desktop, select **Analysis > Remediation > 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 IRM 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.

Testing 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.



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.

- ✓ [Managing issues](#)
- ✓ [Managing Action Plans](#)

MANAGING ISSUES

Creating Issues

You can create issues at all times, for example when a test activity was poorly evaluated.

To create an issue:

1. In the **HOPEX IRM** desktop, select **Test > Remediation > Issues**.
2. Click **New**.
3. Enter a **Name**.
4. In the **Category** field, specify whether the issue:
 - was detected at control assessment
 - was detected when performing tests
 - is generic
5. Specify the **Impact**: enables to qualify the impact of the issue (low, high..)
6. Enter a **Description**.
7. Click **OK**.

Scoping an Issue

You can specify how the issue has been detected.

To define the scope of an issue:

1. In the properties of the issue, expand the **Assessment Scope** section.
2. Connect:
 - a test activity, or
 - one or several assessed controls

Remediating Issues

To remediate an issue, you may create an action plan directly from this issue.

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

Following-Up Issues

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" (whose action plan is closed)
 - "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

You can set up action plans to improve a control that has been considered unsatisfactory ("fail").


Accessing action plans

To access all action plans:

- 1. In the navigation menu, click **Registers > Action Plans**.

To access the action plans you need to work on:

- 1. In the navigation menu, select **My Tasks > Remediation > Action Plans to Implement**.


 *Displays all action plans you need to implement or approve.*


Creating an Action Plan for Testing

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 an Action Plan for Testing](#).*

To specify action plan properties:

1. See [Accessing action plans](#).
2. Open the properties of the action plan.

Action Plan Dashboard

An action plan properties displays the main progress indicators.

- **Progress** (%)
 - ✎ Corresponds to the value of the **Progress Update Percentage** column of the last progress update (**Progression History** section).
- **Timing**
 - On Time
 - Overdue
 - ✎ Corresponds to the value of the **Progress Evaluation** column of the last progress update (**Progression History** section).
- **Result**
 - Failure
 - Success
 - Unknown
 - ✎ Corresponds to the value entered in the **Outcome** field of the **Success Factors and Outcome** section.

General characteristics

You can specify the following information:

- **Name:** action plan name.
- **Priority:** enables indication of a level. Priority can be:
 - "Low"
 - "Medium"
 - "High"
 - "Critical"
- **Owner:** this field is specified by default by 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.
- **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.
- **Nature:** enables definition of whether the action plan is:
 - Corrective
 - Preventive
- **Means:** text description of means required/desired for action plan execution.
- **Description:** enables to specify additional 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.

Responsibilities

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.

Financial assertion

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

Success Factors and Outcome

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

You can enter the **Outcome** of the action plan.

- Unknown
- Failed
- Succeeded

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
- issues

Progress history

The **Progress History** section enables you to follow-up the progress update history by the action plan owner.

See [Indicating Action Plan Progress](#).

Milestones

Milestones are key dates of the action plan.

🔒 *The planned end date is mandatory.*

Attachments

You can attach documents to an action plan or specify an URL.

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

Managing Actions

➡ See also: [Managing Action Plans](#).

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 > Remediation > Action Plans to Implement**.
2. Open the properties of the action plan that interests you.
3. In the **Actions** page, 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.

Action Plan Workflows

➡ See also: [Managing Action Plans](#).

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

☛ See also: [Managing Action Plans](#).

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 > Remediation > Action Plans to Implement**.
2. Open the properties of the action plan.
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
 - Late
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:

- 1. Select **Analysis > Remediation > Follow-Up**.

Access path

Analysis > Remediation > 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
- Mean
- 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.*

REPORTS RELATED TO CONTROLS



This chapter describes reports of the **Analysis** navigation pane. 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.

- ✓ [Control Environment Report](#)
- ✓ [Control Register Reports](#)
- ✓ [Control Execution Reports](#)
- ✓ [Control Assessment Reports](#)
- ✓ [Control Assessment Follow-Up Reports](#)
- ✓ [Control Testing Reports](#)
- ✓ [Issue-Related Reports](#)
- ✓ [IT Regulatory Compliance Reports](#)

CONTROL ENVIRONMENT REPORT

You can choose to display the following elements for a chosen control:

- the risk context
 - business processes
 - organizational processes
 - Applications
 - Org-Units
 - business lines
- the strategic objects impacted by the risk (objectives)
- risk consequences (associated risks)
- preventive controls designed to remediate 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.

- action plans and actions

Access path

Control properties (**Reporting > Control Environment**)

Report parameters

Parameters	Constraints
Control	Mandatory
Control context (business processes, organizational processes, applications, entities, business lines)	Optional
Mitigated Risks	Optional
Deficiencies	Optional
Action plans	Optional
Risk context (business processes, organizational processes, applications, entities, business lines)	Optional

Creating a control environment report

To display a control environment report:

1. In the control properties, select the **Reporting > Control Environment** page.
2. In the **Parameters** section, select the object types you want to display:
 - **Control contexts**
 - **Mitigated risks**
 - **Issues**
 - **Action plans**
 - **Risk contexts**
3. In the **Report 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.

Example



CONTROL REGISTER REPORTS

Control Identification

This report presents distribution of controls according to several perspectives:

- entities
- processes
- control types
- accounts

Access path

Analysis > Control > Identification > Control Identification

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:

- 1 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:

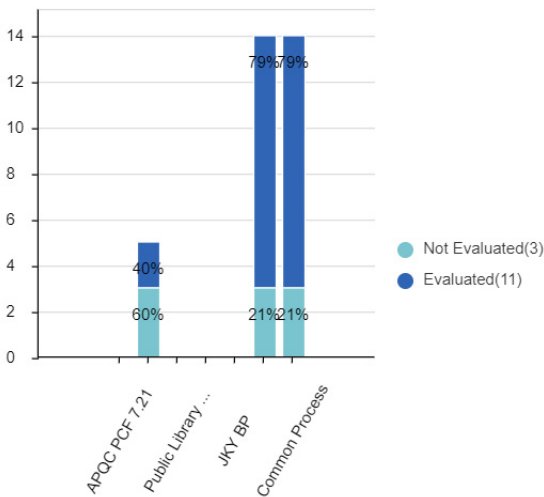
- 1 Click the bar chart bar that interests you.
The list of controls taken into account is presented at the bottom of the edit area.

Bars of the bar chart distinguish assessed controls from those not yet assessed.

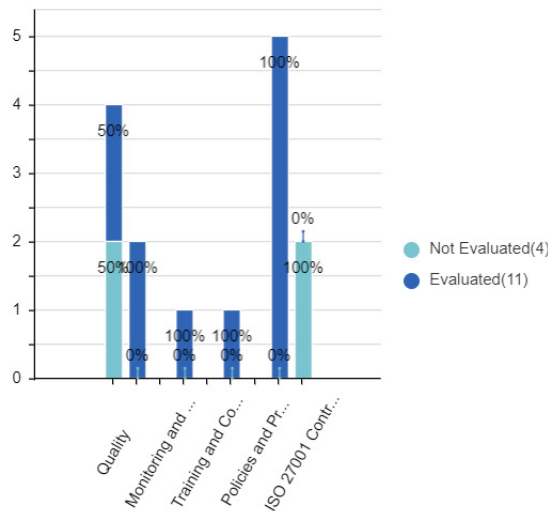
Example

Total number of Controls : 17

Controls by Process



Controls by Control Type



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
End date	Date	Optional All controls created before this date are selected
Context type	The context can be of type: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - Entity - Process - Risk type - Account 	Mandatory Controls to be displayed in matrix rows

Example

	Long Term Procurement	Manage employee information	National taxation
All keys must be stored in a secured location		✓	✓
All sensitive data must be encrypted before saving			
Control all methods of remote access			✓
Do not grant any administrator rights to anybody			✓
Ensure password complexity level			
Sensitive outbound Application Communications are cyphered	✓		

CONTROL EXECUTION REPORTS

- ✓ [Detailed Execution Results](#)
- ✓ [Consolidated Execution Results](#)
- ✓ [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 and example

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.

	Average Percentage of OK Control
 Project Leader	N/A Not Assessed
 MS Azure	N/A Not Assessed
▼  MEGA Airport	 80%
▼  Subsidiaries	 80%
▶  France	 86%
▼  Japan	 89%
▼  Sell Products	 89%
 Segregation of duties	 100%
 Follow-up refused receptions	 100%
 Connection control	 67%

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")

Example

			Jan-2016			Feb-2016		
	Total Nb of Controls	Total Nb of Instances	Nb of Assessed Instances	NB of OK Instances	% OK Instances	Nb of Assessed Instances	NB of OK Instances	% OK Instances
 Belgium	9	9	0	0	0 %	8	0	0 %
 France	16	18	0	0	0 %	12	0	0 %
 Italy	9	9	0	0	0 %	10	0	0 %
 Japan	3	3	0	0	0 %	0	0	0 %
 USA	11	11	0	0	0 %	12	0	0 %

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

Analysis > Controls > Assessment > 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

Analysis > Controls > Assessment > Campaign Results Matrix by Entity

Parameters

Parameters
Campaign
Entity
Entity type

Example

			2014-Q2 - Controls Assessment		
	Total Nb of Controls	Total Nb of Instances	Nb of Assessed Instances	Nb of Pass Instances	% Pass Instances
Belgium	9	9	5	3	60 %
Brazil	1	1	0	0	0 %
Canada	5	5	0	0	0 %
France	16	18	9	7	78 %
Germany	4	4	0	0	0 %
Italy	9	9	7	7	100 %
MEGA Airport	32	86	65	43	66 %

Aggregation Report

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

The following columns are available:

- Design
- Effectiveness
- Control level
- Average percentage of Pass control level

Access path

Analysis > Controls > Assessment > Aggregation Report

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.

CONTROL ASSESSMENT FOLLOW-UP REPORTS

Several reports enable you to follow-up control assessment.

Session Follow-Up

This report enables you to follow-up an assessment session.

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

Analysis > Controls > Follow-up > Session Follow-Up

Parameters

Parameters	Parameter value
Session	Assessment 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
- Percentage of validated questionnaires

A table displays the number of questionnaires by status and respondent.

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 > Controls -> Follow-up > 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, the number of respondents

This tree specifies who has answered what to which question.

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%

Failed Controls

This report displays the number of deficient controls among a list of processes or applications.

Access path

Analysis > Controls > Follow-Up > Failed Controls

Parameters

Parameters enable you to:

- define a start and end date to define the controls to be included (creation date).
- select the processes or applications to be included

Result

The report presents as an horizontal bar chart:

- on the Y axis: the control context objects
- on the X axis: the number of deficient controls according to the last assessment

➡ Deficient controls appear when clicking on a bar of the bar chart.

Report example



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

Plan property page (Reports page)

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

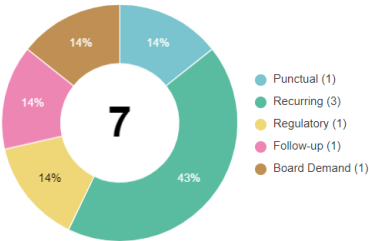
Example

Chapitre généré le 24/07/2024 à 10:24

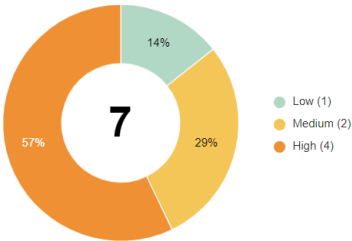
Synthesis Table

All	Planned	Published	Completed	Estimated Workload (Days)	Effective workload (Days)	Average Duration (Days)	Average number of auditors
7	7	7	7	0	0	0	0.0

By origin



By priority



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-RELATED REPORTS

Issue Follow-up Report

The issue follow-up report is presented in the form of a pie chart.

Access path

Analysis > Controls > Remediation > Issue Follow-Up

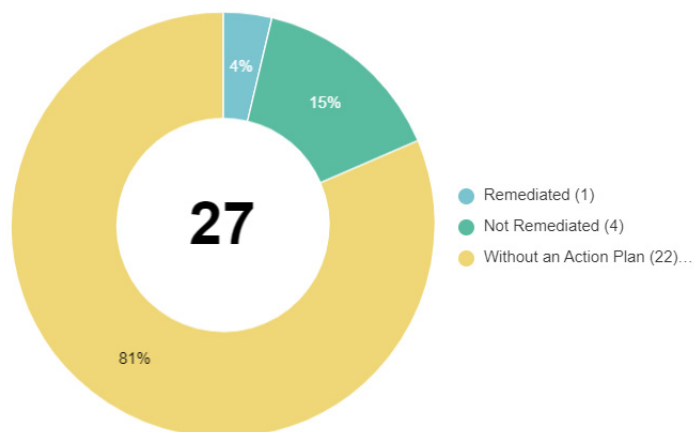
Result

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](#).

Example



“Issues by Impact” Report

This report is a pie chart that groups issues by impact (very low, medium, high, very high)

You can filter results:

- by issue status (open, closed)
- by control type impacted by the issue.

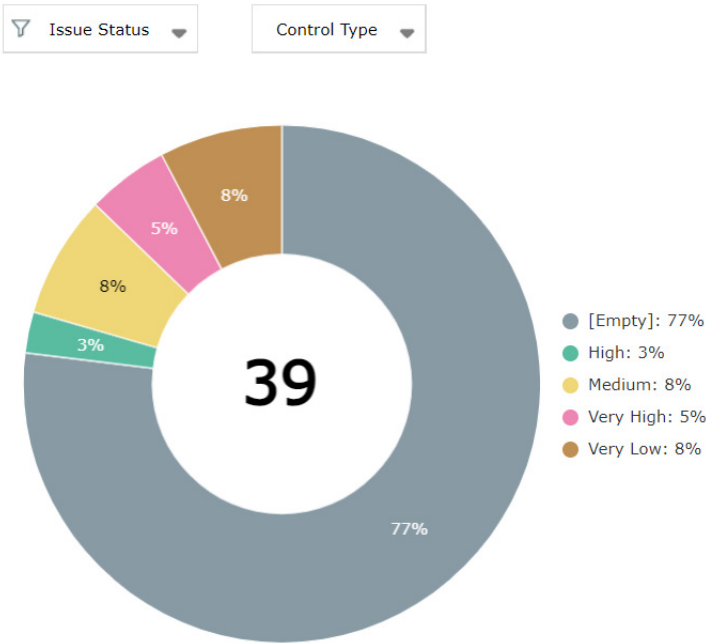
Use case:

- You have connected a number of controls to a control type to meet specific requirements (for example, “IT Compliance”)
- This report enables you to view the issues that impact the control type of interest.

Access path

Analysis > Controls > Remediation > Issues by Impact

Result



HOPEX Enterprise Risk Management



HOPEX ENTERPRISE RISK MANAGEMENT

User Guide

HOPEX V5



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 is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2021

All rights reserved.

HOPEX ERM and HOPEX are 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.

CONTENTS



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

Managing Risks	5
---------------------------------	----------

Risk Management Profiles	6
---	----------

Creating a Risk	7
----------------------------------	----------

Risk characteristics	8
---------------------------------------	----------

General characteristics	8
-----------------------------------	---

Risk Dashboard	8
--------------------------	---

Risk Responsibilities (RACI)	9
--	---

Defining the Scope of a Risk	9
--	---

Analyzing Risks	10
---------------------------	----

<i>Risk types</i>	11
-----------------------------	----

<i>Risk factors</i>	11
-------------------------------	----

<i>Risk consequences</i>	11
------------------------------------	----

Viewing Audit Recommendations Connected to a Risk	12
---	----

Accessing risks	13
----------------------------------	-----------

Accessing All Risks	13
-------------------------------	----

Accessing Orphan Risks	13
----------------------------------	----

Accessing Materialized Risks	13
--	----

Risk Workflow	15
--------------------------------	-----------

<i>Risk validation steps</i>	15
--	----

<i>Validating or rejecting a risk</i>	15
---	----

Assessing Risks	17
----------------------------------	-----------

Risk Assessment Types	18
--	-----------

Direct Assessment or by Campaign	18
--	----

Available Assessment Templates	18
--	----

Prerequisites to Risk Assessment	19
"Risk Assessment by Entity and Process" Template	19
"Risk Assessment by Application" Template	19
Assessing risks directly	20
Direct Risk Assessment Templates	20
<i>Assessed characteristics</i>	20
<i>Respondents</i>	20
<i>Questionnaire</i>	21
Creating a Direct Assessment on a Risk	21
Assessing Multiple Risks Simultaneously	21
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
<hr/>	
Risk Mitigation and Remediation	27
Mitigating Risks	28
Risk Mitigation Strategies	28
Specifying Risk Appetite	28
Implementing Controls	28
Remediating Risks	30
<hr/>	
Risk-Related Reports	31
Risk Environment Report	32
<i>Access path</i>	32
<i>Report parameters</i>	32
<i>Creating a Risk Environment Report</i>	33
Bow-Tie Analysis	35
<i>Access path</i>	35
<i>Example</i>	35
Incident Identification Reports	36
Risk identification	36
<i>Access path</i>	36
<i>Report parameters</i>	36
<i>Report example</i>	37
Aggregation Reports	39
Net Risk by Risk Type	39
<i>Access path</i>	39
<i>Example</i>	39
Risk Heatmap (Aggregated)	40
<i>Access path</i>	40
<i>Report parameters</i>	40
<i>Content of the heatmap</i>	40

Heatmap by Environment	41
<i>Access path.</i>	41
<i>Report parameters.</i>	41
<i>Report example.</i>	42
Assessments per Context	42
<i>Access path.</i>	42
<i>Report parameters.</i>	43
<i>Example.</i>	43
Overall Risk Level by Process	43
<i>Access path.</i>	44
<i>Report parameters.</i>	44
<i>Report example.</i>	44
Overall Risk Level by Entity	44
<i>Access path.</i>	44
<i>Report parameters.</i>	45
<i>Report example.</i>	45
Aggregation Report	45
<i>Access path.</i>	45
<i>Report parameters.</i>	46
<i>Report example.</i>	46
Risk Follow-Up Reports	48
Session Statistics	48
<i>Access path.</i>	48
<i>Parameters.</i>	48
<i>Report example.</i>	49
<i>Result</i>	49
Risk Management Effectiveness Reports.	50
Risk Context Synthesis	50
<i>Access path.</i>	50
<i>Parameters.</i>	50
<i>Report content</i>	50
Risk Reduction	51
<i>Access path.</i>	51
<i>Report parameters.</i>	51
<i>Report example.</i>	51
Coverage & Risks Matrix	52
<i>Access path.</i>	52
<i>Matrix content.</i>	52
Trend Analysis	53
<i>Access path.</i>	53
<i>Report parameters.</i>	53
<i>Report example.</i>	53
<i>Result computation</i>	53

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:

- ✓ [Risk Management Profiles](#)
- ✓ [Creating a Risk](#)
- ✓ [Risk characteristics](#)
- ✓ [Accessing risks](#)
- ✓ [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 IRM 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
IRM Contributor	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 **Registers > Risks > All Risks**.
2. Click **New**.
3. Enter a **Name**
4. (optional) Specify the risk **Identification Mode**
The risk could have been identified from:
 - an "incident database"
 - a "workshop"
 - a "survey"
 - an "audit"
5. (optional) Enter a **Description**
6. Click **OK**.

You can complete risk description through the risk property page.

See:

- [Risk characteristics](#)
- [Risk Workflow](#)

RISK CHARACTERISTICS

☛ To access risks, see [Accessing risks](#).

☛ 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 Environment](#).

General characteristics

To access characteristics of a risk:

- 1 Select a risk from a list of risks or major risks and click **Properties**.

In the property page, you can specify:

- the risk identification **Code**
- the fact that the risk is high level by selecting the **Major 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:

- [Analyzing Risks](#)
- [Risk Responsibilities \(RACI\)](#)
- [Risk Dashboard](#)
- [Defining the Scope of a Risk](#) (scoping risks)

Risk Dashboard

☛ To access risks, see [Accessing risks](#).


A number of indicators are available in the **Characteristics** page of risk properties.


- **Last Assessment:** 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.


- **Residual risk:** Average of the net risk obtained from the last assessment session. All the contexts for which the risk was assessed

during the last assessment session are considered (e.g. entities, processes, applications...) and the average is computed.

 *The residual (or 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.
- **Forecast risk:** represents the residual risk forecast for the year to come (average residual risk)

Risk Responsibilities (RACI)

 To access risks, see [Accessing risks](#).

Risk properties include a **Responsibilities** section to define the different persons responsible for risk management. For more details, see [Responsibilities \(RACI\)](#).

Note that the Risk Assessor, who answers risk-related questionnaires, is to be specified in the properties of the entity connected to the risk(Entities / Processes/).

 For more details, see:

- [Prerequisites to Risk Assessment](#)
- [Specifying responsibilities within an entity](#).

See also:

- [Defining the Scope of a Risk](#)
- [Analyzing Risks](#)
- [Risk Dashboard](#)

Defining the Scope of a Risk


Contextualizing a risk consists in defining its scope.

To define the scope of a risk:

- In the risk properties, expand the **Scope** section.

The scope can consist of different types of objects:

- **Business Processes** and **Organizational Processes** exposed to the risk. 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.

- **Operations**



An operation is an elementary step in an organizational process. It corresponds to the intervention of an entity within the organization.

- **Entities** concerned by the risk. 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 Environment](#).

- **Objectives** expected related to risk management.



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.

- **Applications.** See [Managing Applications](#).



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

- **Business Lines:** 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.

Analyzing Risks

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. See [Accessing risks](#).
2. Select a risk and open its properties.

3. 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**



*The incidents related to the risk appear in the **Incidents** page of the risk properties.*

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 **Environment > Risks > Risk Types**.
2. Click **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:

1. See [Accessing risks](#).

2. In the risk properties, **Analysis** section, **Risk Consequences** tab, click **New**.

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

Viewing Audit Recommendations Connected to a Risk

To view risk-related recommendations:

1. See [Accessing risks](#).
2. In the properties of a risk, select the **Audits** page.

🔑 *This page is available if you have **HOPEX Internal Audit**.*

This page contains:

- Recommendations that have the risk in their scope
- Recommendations connected to a finding with the risk in its scope

For more details on risks and recommendations within the framework of an audit, see:

- [Defining and Assessing Risks](#)
- [Sending Recommendations](#)

ACCESSING RISKS

Accessing All Risks

To access risks:

- 1 In the **HOPEX IRM** desktop, select **Registers > Risks**.

For each risk, you can access the following information:

- **Code**
- **Major Risk** (is it a major risk or not?)
- **Entities**
- **Last assessment** (date)
- **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.

- **Residual risk**



The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

- **Open Incidents** (number of)
- **Forecast Risks (number of)**
- **Action Plans** (number of)

The **Status** enables you to distinguish between risks that were **Submitted** (and need to be reviewed) from those that were **Validated**.

Accessing Orphan Risks

To access risks that are not connected to any contexts:

- 1 In the **HOPEX IRM** desktop, select **Registers > Risks > Orphan Risks**.

This list displays all the risks that have no impact on the organization. These risks are not connected to any processes, applications, entities or business lines.

To define appropriately the impact of a risk:

- 1 Fill in the **Scope** section in the **Characteristics** page of its properties.

Accessing Materialized Risks


 A materialized risk is a risk for which an incident occurred.

To access risks that materialized through an incident:


- 1 In the **HOPEX IRM** desktop, select **Registers > Risks > Materialized Risks**.

For each risk, the following information appears in columns:


- **Net Loss**

 The value displayed here is the sum of net losses of all incidents declared for the risk.


- **Incidents Declared** (number of)
- **Latest Incident** (date)
- Associated **Entities**
- **Last Assessment** (date)
- **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.

- **Residual risk**

 The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

- **Forecast risk**

 Forecast risk represents the residual risk forecast for the year to come.

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](#).

Risk validation steps

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) must **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.

Validating or rejecting a risk

To validate or reject a risk:

1. In the navigation menu, select **My tasks > Review > Risks to Review**.
2. Select the risk(s) to validate/reject and use the **Workflow** button to select the appropriate transition.

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.

- ✓ [Risk Assessment Types](#)
- ✓ [Prerequisites to Risk Assessment](#)
- ✓ [Assessing risks directly](#)
- ✓ [Viewing and Analyzing Risk Assessment Results](#)

RISK ASSESSMENT TYPES

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

- impact
- likelihood
- risk control level

Direct Assessment or by Campaign

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 [Starting an Assessment Campaign](#).

Results of risk assessment can be displayed in dedicated reports that make it easier to analyze the assessed risks. For more details, see [Risk-Related Reports](#).

➡ See also: [Prerequisites to Risk Assessment](#).

Available Assessment Templates

HOPEX offers two different templates to assess risks from two perspectives:

- Risk Assessment by Entity and Process
- Risk Assessment by Application

➡ See also: [Prerequisites to Risk Assessment](#).

PREREQUISITES TO RISK ASSESSMENT

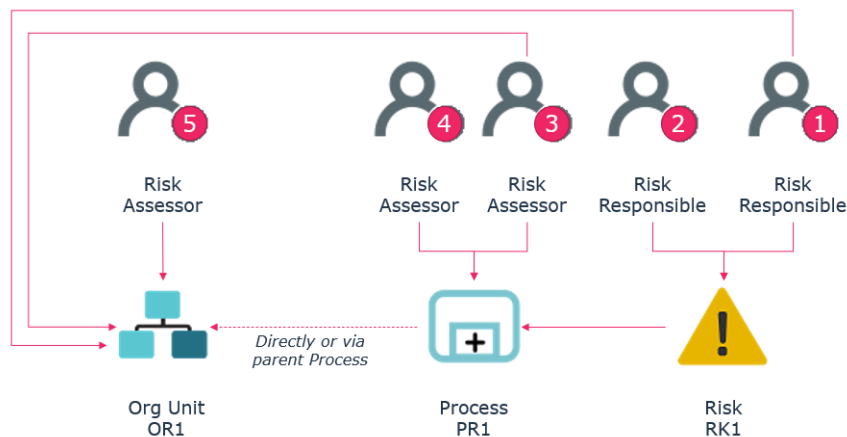
“Risk Assessment by Entity and Process” Template

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

- connected risks to at least one entity/ one business process
- specified one or several respondents in the entity/process properties (Risk assessor)

Respondents to risk-related questionnaires can be defined on:

- entities
- processes connected to entities (directly or via a parent process)
- risks connected to processes (directly or via a risk)



Respondent definition logics

“Risk Assessment by Application” Template

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

- connected risks to at least one application
- specified one or several respondents in the application properties (Application owner)

ASSESSING RISKS DIRECTLY

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

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

- in risk properties: [Creating a Direct Assessment on a Risk](#)
- globally, using a multiple assessment table: [Assessing Multiple Risks Simultaneously](#)

Direct assessment is carried out for all entities or applications available in the **Scope** section of the risk properties.

➡ See also: [Starting an Assessment Campaign](#).

Direct Risk Assessment Templates

HOPEX IRM provides risk assessment templates in the context of the following objects:

- entity and process
- application

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
- Probability
- Control Level



Risk control level enables characterization of control efficiency in mitigating the risk.

- Residual risk



The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

Respondents


Respondents can be:

- Risk **Responsible** users (on risks), or
- **Risk Assessors** (on entities or processes)

➡ It is possible to define several respondents.


➡ For more details, see [Prerequisites to Risk Assessment](#).

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
- Probability
- Control Level

 Risk control level enables characterization of control efficiency in mitigating 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 **Evaluation** page.
3. Click **New Assessment**.


 A page offering to select context(s) appears if several contexts are available for the risk concerned.

4. Assign characteristics values for the risk being assessed:
 - **Impact**: the impact of the risk when it occurs.
 - **Likelihood**: the probability that the risk will occur.

 If the risk has already been assessed, impact and likelihood values from the last assessment are suggested. You can modify these values for the new assessment.

- **Control Level**

 Risk control level enables characterization of control efficiency in mitigating the risk.

 If the risk has already been assessed, a Control Level value is also suggested. For more information, see [Risk Control Level](#).

5. Specify the **Assessment Date** if necessary.
 6. Click **OK**.
- An assessment is created.


Assessing Multiple Risks Simultaneously

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, select **Assessment > Direct Assessment > Risk Multiple Assessment Table**.




2. Click **Launch Multiple Assessment**.
3. In the window that appears, select the **Assessment template**:
 - "Risk Assessment by Entity and Process"
 - "Risk Assessment by Application"
4. In the displayed tree, select the objects that define the assessment context (entity or application, depending on the selected template).

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


To help you choose the risks to be assessed, the following information is displayed in columns:

- **Last Assessment**
- **Residual Risk**
- **Open Incidents**
- **Forecast Risk**


 This information is also available in the risk dashboard. For more details, see [Risk Dashboard](#).


	Assessment Freshness	Net Risk	Open Incidents	Forecast Risk
  MyCompany				
   World@Hand Corporation				
  Corporate Headquater				
   Regional Headquater				
  Car Rental Department				
   HR Department				
  Architecture lacks flexibility	None	None	0	None
  Forged invoice (purchase)	None	None	0	None
  Goods receipt inconsistant w...	None	None	0	None

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

 If you deselect a node of a branch, only the child elements of this branch are deselected.

5. Click **OK**.

 If assessments have already been carried out, the most recent assessment values are presented in columns.
6. For each assessed object, select values:
 - **Impact**: characterizes impact of the risk when it occurs.
 - **Likelihood**: characterizes probability that the risk will occur.

 Values entered for impact and likelihood during the last assessment are displayed.
 - **Control Level**: gives an overall assessment of risk control level.
7. When you have finished, 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) 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 IRM functional administrator only can delete assessment results (that is to say assessment nodes).*


*To delete an assessment node, select it and click **Delete**.*

For each assessment node the following values are computed:

- 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.*

- residual risk

 *The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.*

Generating Reports on Assessments

Instant reports

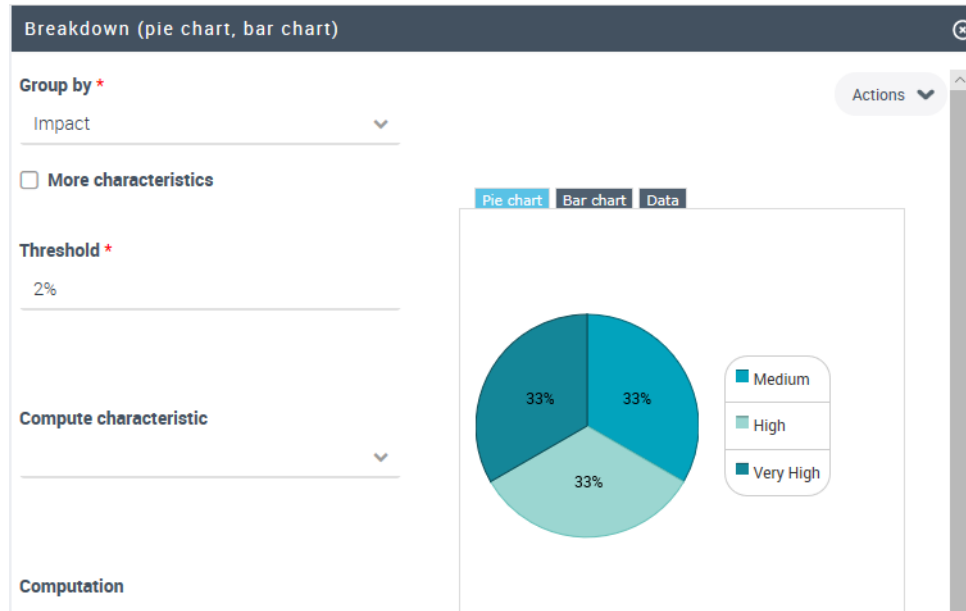
Instant reports offer a statistical graphic analysis of data. You can generate instant reports on a selection of assessments in order to view certain data graphically or to compare the assessments for specific characteristics.

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 [Risk-Related Reports](#).



RISK MITIGATION AND REMEDIATION



HOPEX IRM enables to define risk-mitigating strategies and to implement action plans to remediate risks.

- ✓ [Mitigating Risks](#)
- ✓ [Remediating Risks](#)

MITIGATING RISKS

To specify risk-mitigating choices:

1. In the **HOPEX IRM** desktop, select **Registers > Risks > All Risks**.
2. In the properties of a risk, select the **Mitigation** page.
3. Define your risk management strategy and implement preventive, detective and corrective controls.

Risk Mitigation Strategies

There are various possible solutions to face risks.


- **Acceptance**
This is the strategy of risk management that consists of accepting the risk having considered its consequences. As long as no desire to remediate the risk is expressed, this strategy will not protect the organization against the risk.
- **Reduction**
Risk frequency can be reduced by installing additional controls, or the impact of its consequences can be reduced if the risk occurs.
- **Transfer** (sub-contractor)
The risk can also be shared with other partners, in particular when they have greater skills in controlling the risk.
- **Insurance**
Complementing all previous approaches, it is often necessary to seek assurance, in particular for risks of low frequency but with high impact.

The different scenarios possible are analyzed to weigh up their positive and negative aspects, with a view to selecting a scenario compatible with the risk control level in question.


Specifying Risk Appetite

To specify the level of risk accepted by the organization:

1. In the risk properties, select the **Mitigation** page.
2. Specify the **Risk Appetite**.

 *Risk appetite is the level of risk an organization is ready to accept to reach its objectives, before any measure is taken to mitigate the risk.*

Implementing Controls

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

To define controls on the risk:

1. In the risk properties, select the **Mitigation** page.
2. In the **Controls** section, define corrective or preventive controls.
 - ☛ *The control nature (corrective or preventive) is to specified in the control properties.*
 - *Implementation of prevention controls to reduce risk frequency and impact can be a solution for risk reduction.*
 - *Implementing corrective controls enables to bring risk level to an acceptable level.*

REMEDIATING RISKS

To specify action plans that enable to prevent or treat the risk:

1. In the **HOPEX IRM** desktop, select **Registers > Risks > All Risks**.
2. In the properties of a risk, select the **Action Plans** page.



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 [Managing Action Plans](#).

This page contains the list of implemented action plans: 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.

A workflow is automatically created at creation of the action plan. For more details, see [Action Plan Workflows](#).

RISK-RELATED REPORTS



Different report templates proposed as standard by **HOPEX IRM** enable analysis of controls and risks.

- ✓ Risk Environment Report
- ✓ Risk Type Analysis Breakdown Report
- ✓ Bow-Tie Analysis
- ✓ Incident Identification Reports
- ✓ Aggregation Reports
- ✓ Risk Follow-Up Reports
- ✓ Risk Management Effectiveness Reports

RISK ENVIRONMENT REPORT

 This report is available to all ERM profiles.

You can choose to display the following elements for a chosen risk:

- the risk context
 - business processes
 - organizational processes
 - Applications
 - Org-Units
 - business lines
- the strategic objects impacted by the risk (objectives)
- risk consequences (associated risks)
- preventive controls designed to remediate 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.

- action plans and actions

Access path

Risk properties (**Reporting > Risk Environment**)

Report parameters

Parameters	Parameter type	Constraints
Risk	1 risk	Mandatory
Risk context (business processes, organizational processes, applications, entities, business lines)	Check Box	Optional
Objectives	Check Box	Optional
Associated 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 object types you want to display.

Credit card risk

Reporting

Risk Environment

Parameters

☒ Risk context (Business Processes, Organizational Processes, Applications, Org-
units, Business Lines)

☐ Objectives

☐ Target Risks

☐ Controls

☐ Incidents

☐ Findings

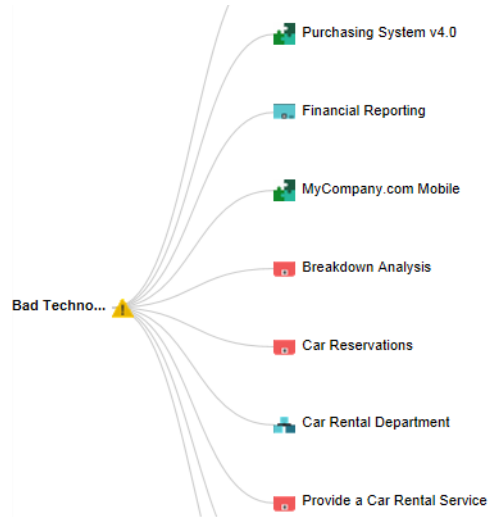
☐ Action Plans

☐ Actions

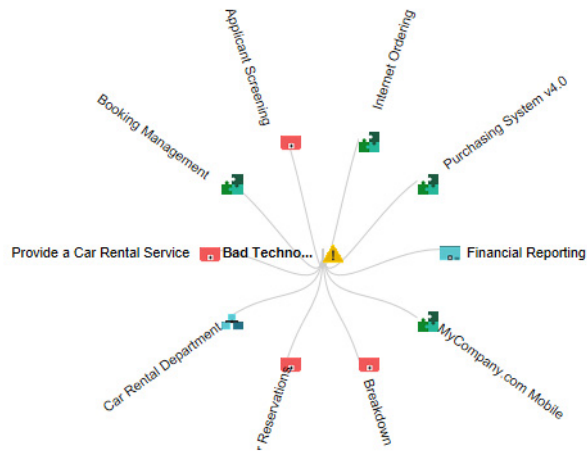
Display*

Horizontal

3. In the **Report 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.

RISK TYPE ANALYSIS BREAKDOWN REPORT

The "Risk type impact analysis (breakdown)" report enables you to view the impacts of the selected risk type.

To access this breakdown report:

1. In the navigation menu, select **Analysis > Other**.
2. Click **New**.
3. Select the "**Risk type Impact analysis (breakdown)**" report template.
4. Click **Next**.
5. Connect a **Risk type**.
6. Click **Connect** and **OK**.
7. Open the report created.

Risk Type Impact analysis (Breakdown) ⓘ



Levels All ▾ Show Risk x ▾

Damage to Phy Assets

- ⚠ IT Access to Purchase Order is impossible
- ⚠ Purchase order not conforming to internal management rules
- ⚠ Bad Technology Choices

Information security

- ⚠ Firewalls
- ⚠ Stakeholder turnover

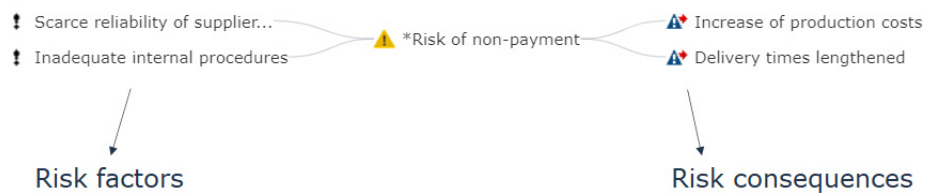
BOW-TIE ANALYSIS

Bow-tie analysis enables to display risk causes and consequences.

Access path

Risk properties (**Reporting** > **Bow-Tie Analysis**)

Example



INCIDENT IDENTIFICATION REPORTS

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.

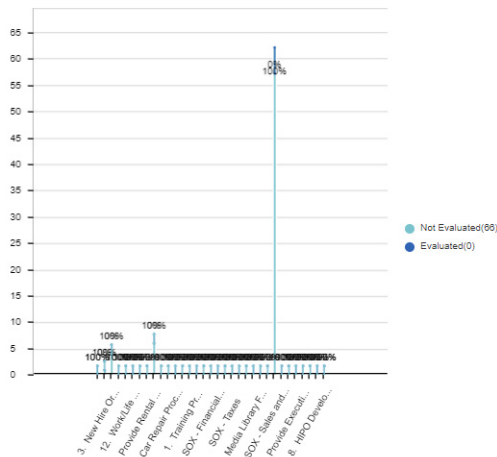
Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default
Scope risk type	Risk type	Not mandatory.
Scope entities	entity	Not mandatory.
Scope processes	process	Not mandatory.
Scope objectives	objectives	Not mandatory.

Report example

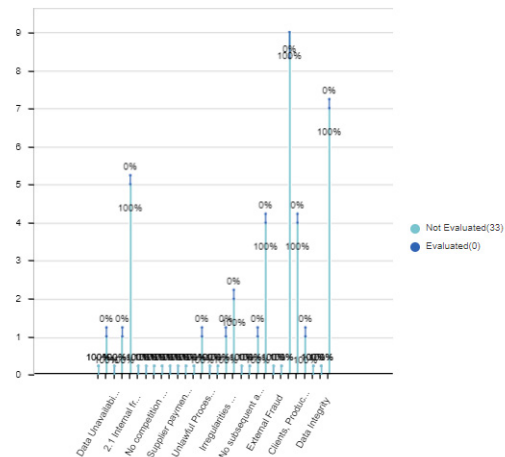
The upper part of the report presents distribution of risks according to the following criteria:

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

Risks per Process



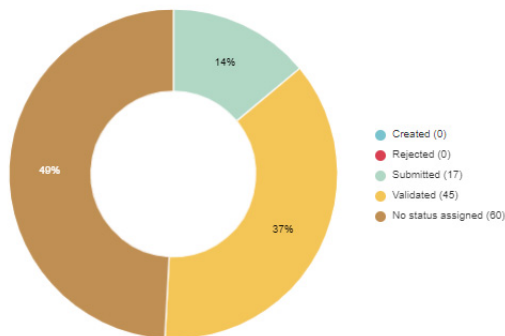
Risks per Risk Type



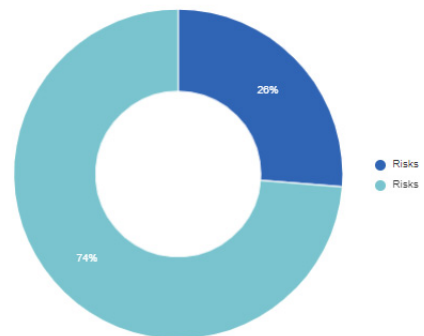
The lower part of the report presents distribution of risks on the following criteria:

- 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.

Risks per Status




Risk Mitigation



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

- 1 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

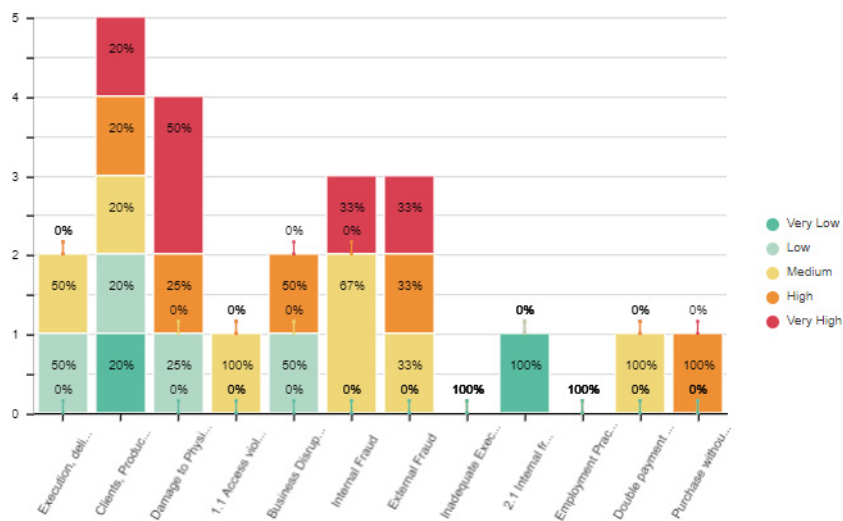


The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.

Access path

Analysis > Risks > Aggregation > Net Risk by Risk Type

Example



Risk Heatmap (Aggregated)

This report enables the Risk Manager as well as all contributors to display the impact and the likelihood of a set of risks. The objective is to view the risks which require attention.

☛ *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

This heatmap displays the aggregated values of risks without risk duplication (as context is not taken into account).

		Impact				
		Very Low	Low	Medium	High	Very High
Likelihood	Certain	0	0	2	1	4
	Probable	2	3	4	2	0
	Likely	1	4	3	0	0
	Possible	2	3	0	0	0
	Rare	4	3	2	0	0
		Control Level				
		Effective	Few observations	Frequent observations	Ineffective	Inexistent
Inherent Risk	Very High	0	1	0	0	4
	High	2	0	0	3	3
	Medium	0	3	3	1	3
	Low	4	2	1	1	5
	Very Low	4	0	0	0	0

Heatmap by Environment

This report displays distribution of risks according to different criteria:

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

Access path

Analysis > Risks > Aggregation > Heatmap by environment

Report parameters

This consists of defining report input data.

Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default.
List of risk types	Risk type	Not mandatory.
List of org-units	entity	Not mandatory.
List of processes	process	Not mandatory.
List of objectives	objectives	Not mandatory.
List of control systems	Control systems	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).

☛ To activate control systems, from the main menu select **Settings > Options** then **Compatibility > HOPEX Solutions > Control Systems activation**.

Report example

Inherent Risk		Impact				
Likelihood		Very Low	Low	Medium	High	Very High
	Certain	0	0	0	0	0
	Probable	0	0	0	0	0
	Likely	0	0	0	0	0
	Possible	0	0	0	0	0
	Rare	0	0	0	0	0

Residual Risk		Control Level				
Inherent Risk		Effective	Few observations	Frequent observations	Ineffective	Inexistent
	Very High	0	0	0	0	0
	High	0	0	0	0	0
	Medium	0	0	0	0	0
	Low	0	0	0	0	0
	Very Low	0	0	0	0	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

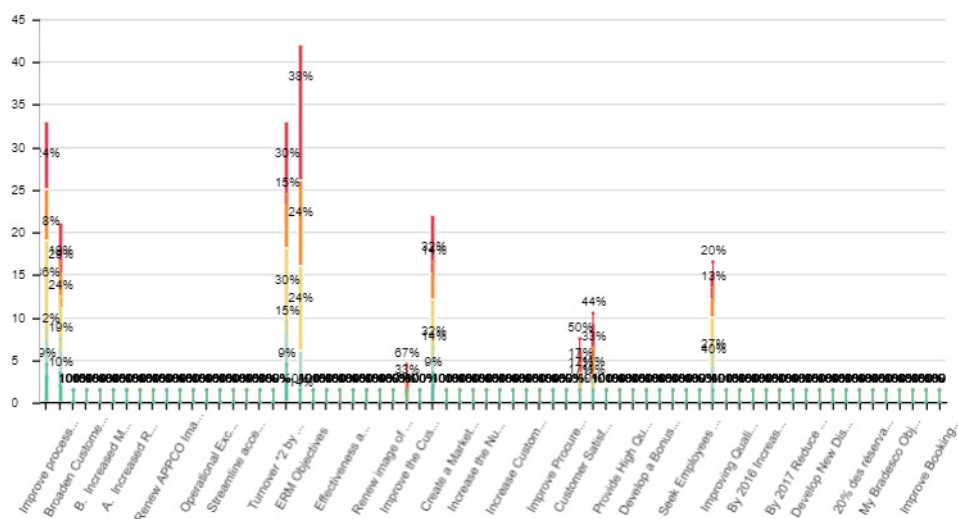
Analysis > Risks > Aggregation > Assessments per Context

Report parameters

Parameters	Parameter type
Begin Date	Date
End date	Date
Context type	Business processes Objective Org Unit Risk Type

Example

Risks assessment per Objective



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	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default.
List of business processes	Business processes	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	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default.
Number of Entities	Entities	Not mandatory.

Report example

Action Plan	Current Average Net Risk Level-1	Max Risk Level	Min Risk Level	Objectifs	Risk	Target Average Risk	
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:

- in rows: all the risks in the scope of the Risk Manager
- in columns: the controls whose purpose is to mitigate these risks

	Approval of needs control	Debit level	Follow-up 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							
Fraud: unregistered call for tender							
Insufficient budget							
Insufficient market analysis							

Risk mitigated by a control
 Inherent Risk / Control Level
 Risk not mitigated by any control

When a risk is mitigated by a control and an assessment has already been made, the values "Inherent risk/Control Level" are displayed at the intersection of the risk and the control. The values correspond to those obtained during the last risk assessment.

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.

Risk control level enables characterization of control efficiency in mitigating the risk.

Trend Analysis

This report displays:

- Risk net average over the last three years
- Next year Forecast for the year to come.

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 computation

Computation method

Forecast Risk =

Net Risk Year N + (Net Risk Year N – Net Risk Year N-2)/2)

Internal values

Value name	Internal value
Very Low	1
Low	16
Medium	81
High	256
Very High	625

Example

Forecast Risk = High + ((High - Very High)/2)

Forecast Risk = 256 + ((256 - 625)/2)

Forecast Risk = 71,5 (rounded off to the nearest threshold = 81)

Forecast Risk = Medium

A stylized, light blue globe with a textured, watercolor-like appearance. The continents are represented by darker blue shapes. The globe is centered on the Atlantic Ocean, showing parts of North and South America on the left and Europe and Africa on the right.

HOPEX LDC

HOPEX LDC

User Guide

HOPEX V5



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 is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2021

All rights reserved.

HOPEX LDC and HOPEX are 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.

CONTENTS



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

Collecting Incidents	5
---------------------------------------	----------

Connection Profiles to HOPEX LDC	6
---	----------

Managing Incidents	7
-------------------------------------	----------

Accessing incidents	7
-------------------------------	---

Creating incidents	7
------------------------------	---

Specifying Incident Characteristics	8
--	----------

Recording Incident-Linked Amounts	9
--	----------

Accessing Incident Financial Analysis	9
---	---

Entering a Loss	9
---------------------------	---

Defining scope of a loss	10
------------------------------------	----

Entering Gains	11
--------------------------	----

Recording Recoveries	12
--------------------------------	----

Recording Provisions.	12
-------------------------------	----

Viewing Computed Amounts Related to the Incident.	13
---	----

<i>Gross Loss</i>	13
-----------------------------	----

<i>Gross actual loss</i>	13
------------------------------------	----

<i>Recoveries</i>	13
-----------------------------	----

<i>Net Loss</i>	13
---------------------------	----

<i>Net Actual Loss</i>	13
----------------------------------	----

Accessing the Incident Register	14
--	-----------

<i>Viewing open incidents</i>	14
---	----

<i>Viewing all incidents</i>	14
--	----

<i>Viewing macro-incidents</i>	14
--	----

<i>Viewing incidents without impacted elements</i>	15
--	----

Analyzing Incidents	16
--------------------------------------	-----------

Incident Qualitative Analysis	16
---	----

<i>Risks and controls</i>	16
-------------------------------------	----

<i>Incident priority</i>	16
------------------------------------	----

<i>Incident Impact</i>	16
----------------------------------	----

<i>Risk factors</i>	17
<i>Risk consequences</i>	17
Incident scope	17
Incident Impact Analysis	18
Managing Macro-Incidents	20
Connecting Incidents to Macro-Incidents	20
Creating a Macro-Incident	20
Analyzing Macro-Incidents	21
<i>Incidents connected to the macro-incident</i>	21
<i>Macro-incident amounts</i>	21
<i>Losses evolution report</i>	21
Incident Management Process	22
Incident Management Process General Description	22
Incident Management Process Steps	22
<i>Submitting incidents</i>	22
<i>Validating incidents</i>	22
<i>Closing incidents</i>	23
<hr/>	
Reports Related to Incidents	25
Loss Analysis Reports	26
Incident and Loss Distribution	26
<i>Access path</i>	26
<i>Report parameters</i>	26
Incident and Loss Evolution by Month	27
<i>Access path</i>	27
<i>Report parameters</i>	27
<i>Results</i>	28
Incident and Loss Evolution by Risk Type	28
<i>Access path</i>	28
<i>Report parameters</i>	28
<i>Results</i>	29
Back Testing Reports	30
Back Testing Matrix	30
<i>Access path</i>	30
<i>Report parameters</i>	30
Back Testing By Risk Type	31
<i>Access path</i>	31
<i>Report parameters</i>	31
Back Testing by Business Line	31
<i>Access path</i>	31
<i>Report parameters</i>	32
Capital Calculation Reports	33
Loss Distribution Matrix	33
<i>Access path</i>	33
<i>Report parameters</i>	33
BIA Approach	34
<i>Access path</i>	34
<i>Report parameters</i>	34

TSA Approach35

Access path.35

Report parameters.35

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 IRM Manager / Incident and Loss Manager can analyze the incident 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.

- ✓ [Connection Profiles to HOPEX LDC](#)
- ✓ [Managing Incidents](#)
- ✓ [Specifying Incident Characteristics](#)
- ✓ [Accessing the Incident Register](#)
- ✓ [Analyzing Incidents](#)
- ✓ [Managing Macro-Incidents](#)
- ✓ [Incident Management Process](#)

➤ *For more information on how to treat incidents, see the documentation concerning action plans.*

CONNECTION PROFILES TO HOPEX LDC

To connect to **HOPEX**, see [Connecting to HOPEX](#).


Profiles	Desktop	Tasks
Incident and Loss Manager (or IRM Manager)	HOPEX IRM	<p>Prepares the work environment and create elements required for management of incidents and losses.</p> <p>Describes the environment: entities and organizational processes, regulatory environment, IT resources</p> <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




Accessing incidents

To access incidents:

- 1. (HOPEX IRM desktop), select **Registers > Incidents > All Incidents**.
 See also [Accessing the Incident Register](#).
- 2. (IRM Contributor profile) Select **Incidents**.







Creating incidents

To create an incident:

1. See [Accessing incidents](#).
2. Click **New**.
 With the "IRM Contributor" profile, click **New Incident** from the Home Page.
3. In the properties of the incident, enter:
 - Its **Name**
 - the **Declarant's entity**
 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.
 - the **Detection date**
 - the **Occurrence Date**
 - a **Description**.
 For more details on these characteristics, see [Specifying Incident Characteristics](#).
4. Click **OK**.

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 **Characteristics** page of the incident properties, fill in the following fields:
 - **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](#).*
 - **Status:** Indicates current status of the incident in the incident management process.
 *The **Status** is grayed because it is managed automatically by the associated incident workflow. For more details, see [Incident Management Process](#).*
 - **Declaration Date, Detection Date, and Occurrence Date:** 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.*
 - **Nature:** you may enter the nature (financial or not) of the incident.
 - **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.*
 - **Description** is a comment describing the incident.


See also: [Recording Incident-Linked Amounts](#)


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.*

See also: [Specifying Incident Characteristics](#).

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 Computed Amounts Related to the Incident](#).

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 Analysis** 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.
The new loss appears in the list.
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. Click the button next to the **Amount** field to select the loss currency.
 - ☛ 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. It is however possible to enter actual 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.

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 Analysis** 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 [The Compliance 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 Analysis** 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 Analysis** 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.

- To specify information specific to a provision, proceed in the same way as for a gain.
 For more details, see [Entering Gains](#).

Viewing Computed Amounts Related to the Incident

To view computed amounts related to the incident:

- See [Accessing incidents](#).
- 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).
 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 valued indications on incidents:

- Gross Loss

Sum of losses (including estimated losses) - Gains
- Gross actual loss

Sum of losses (excluding 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 REGISTER

To manage incidents:

- 】 Click **Registers > Incidents**.
Tiles enable to access incidents through different criteria. Lists display columns to sort incidents.

Viewing open incidents

Registers > Incidents > Open incidents

Open incidents are incidents that were validated by the Risk Manager.

Viewing all incidents

Registers > Incidents > All Incidents

Incidents are grouped by status, which enables to view those that require your attention (for example incidents to be validated, or to be closed).

- Project
- To be validated
- Validated
- Rejected
- Closed

The following columns are displayed by default for each incident:

- Code
- Declared by
- Declaration date
- Occurrence date
- Declarant's entity
- Impact

☛ This column enable to view declared incidents with High Impact.

- Net Actual Loss
- Action Plans: displays the number of action plans in progress related to the incident.

☛ You can display additional columns to enable you to filter incidents according to specific criteria (for example to view incidents related to a specific macro-incident).

Viewing macro-incidents

Registers > Incidents > Macro-Incidents

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](#).

The following columns are displayed by default:

- Code
- Net Actual Loss
- Validated Incidents (number of)
- First Occurrence
- Last Occurrence
- Last Occurrence Declarant

You may also display the following columns:

- Description
- Gross actual loss
- Recoveries

Viewing incidents without impacted elements

Registers > Incidents > Orphan Incidents

This list displays the elements that have no impact on the organization (without context).

To define (context) elements impacted by an incident:

- 】 Open the properties of an incident and select **Characteristics > Scope > Incidents**.

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** page expand the **Qualitative Analysis** section.

Risks and controls

To connect an incident to a risk and a control:

1. Click the arrow at the right of the **Materialized Risk** field and select **Connect Risk**.
2. Select the risk that interests you and click **OK**.



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

3. Click the arrow at the right of the **Failed Control** field and select **Connect Control**.
4. Select the control that interests you and click **OK**.



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

Incident priority

To qualify the priority of an incident:

1. In the property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Specify the **Priority** characterizing the incident relative importance.
 - "High"
 - "Medium"
 - "Low"

Incident Impact


To specify the impact of an incident:

1. In the incident properties, select the **Financial Analysis** page.

2. Specify the **Impact** characterizing impact of the incident on environment elements.
 - "Very High"
 - "High"
 - "Medium"
 - "Low"
 - "Very Low"

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 property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Select the **Risk Factor** tab and click the **Connect** button.
3. Select the risk factor associated with the incident.
4. Click **OK**.

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 property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Select the **Risk Consequence** tab and click the **Connect** button.
3. Select the risk consequences associated with the incident.
4. Click **OK**.

Incident scope

To specify the scope of an incident:

1. See [Accessing incidents](#).
2. In the property page of Incident, select the **Characteristics** page and 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

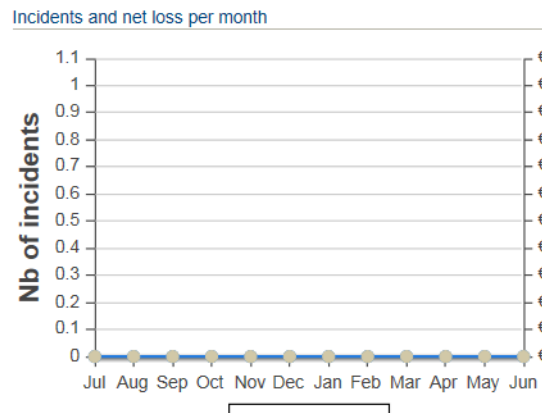


An application is a set of software tools coherent from a software development viewpoint.

Incident Impact Analysis

HOPEX IRM offers the possibility to analyze, from several perspectives, the distribution of incidents linked to an element of 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 willful incident in a building can have consequences on several business lines or organizational units.

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**.
5. Select the macro-incident that interests you and click **OK**.

☛ Incidents are visible in the **Incidents** page of the macro-incident.

Creating a Macro-Incident

☛ This feature is proposed only to Risk Managers and Incidents and Losses Managers.

To create a macro incident:

1. Select **Registers > Incidents > Macro-Incidents**.
2. Click **New**.
3. In the macro-incident properties, select the **Characteristics** page.
4. Specify the following fields:
 - **Name**
 - **Description**: comment concerning the macro-incident.
5. 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- instance, the fields **Validated Incidents**, **First Occurrence** and **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 incident approver receives an e-mail and the new incident appears with status "Submitted".
 To specify the incident approver, see [Specifying responsibilities within an entity](#).
- When an incident has been submitted by its declarant, the incident approver can **Request modifications** of the incident which takes status "Project".
A e- mail is sent to the incident declarant.
- 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 also [Incident Workflow](#) workflow definition diagram.

Incident Management Process Steps

Submitting incidents

When you have specified information concerning the incident, you can submit it for approval.

To submit an incident:

1. See [Accessing incidents](#).
2. Select the incident you want to submit and click **Workflow > Submit**.

If the incident declarant has role "Incident Approver", 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. Click **My Tasks > Review > Incidents to Review**.
The list of incidents for which you are responsible appears.
2. Select the incident you want to handle and click **Workflow**.
3. Select one of the following transitions:
 - **Validate** the incident status turns to "Validated".
 - **Reject**

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. Click **Registers > Incidents > Open incidents**.
2. Select the incident you want to submit and click **Workflow > 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.

➤ See also: [Reports Related to Incidents](#).

- ✓ [Loss Analysis Reports](#);
- ✓ [Back Testing Reports](#);
- ✓ [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 scope.

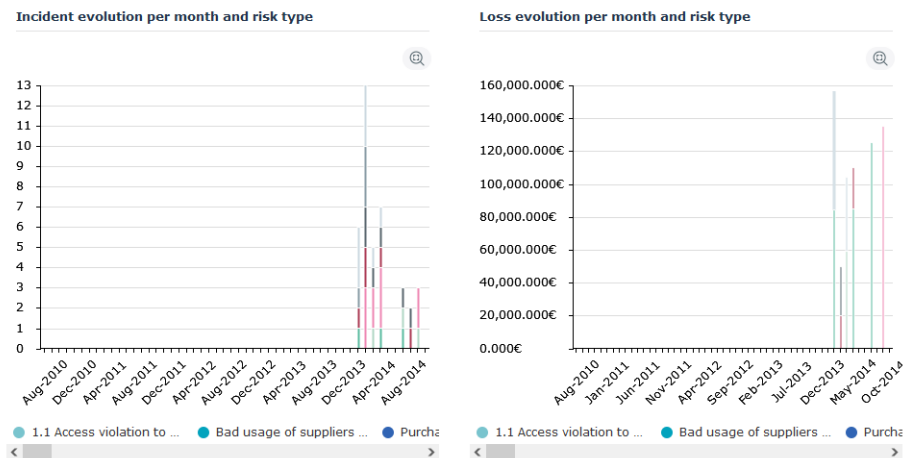
Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. The user currency is used by default.
Warning threshold	Real	Takes into account the incidents whose loss amount is higher than this threshold.
Begin Date	Date	One year before the current date (by default)
End date	Date	Current 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.

LDC - Incident and Loss Evolution per Risk Type ⓘ



➡ 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	Integer	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	Integer	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	Integer	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.

