

HOPEX LDC

User Guide

HOPEX V2R1



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 - 2018

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
---------------------------	----------

Introduction	5
-------------------------------	----------

Incident Management Process	6
<i>Declaring incidents</i>	6
<i>Analyzing incidents</i>	6
<i>Remediating Incidents</i>	6
<i>Obtaining follow-up reports</i>	6
Connecting to HOPEX LDC	7
Connecting to the solution	7
Profiles of HOPEX LDC	7
Interface Presentation	9
About This Guide	10
Guide Structure	10
Additional Resources	10
Conventions Used in the Guide	11
<i>Styles and formatting</i>	11

Incident and Loss Administration	13
---	-----------

Preparing Financial Amount Management	14
Managing Multiple Currencies	14
<i>Principle of use</i>	14
<i>Defining Central Currency</i>	14
<i>Defining Local Currency</i>	15
<i>Defining user local currency</i>	15
<i>Define exchange rates</i>	15
Managing Threshold Amounts	16

Collecting Incidents	17
Declaring Incidents	18
<i>Creating incidents</i>	18
<i>Specifying incident characteristics</i>	18
<i>Duplicating incidents</i>	19
Recording Incident-Linked Amounts	20
Accessing Incident Financial Analysis	20
Entering a Loss	20
Defining scope of a loss	21
Entering Gains	22
Recording Recoveries	23
Recording Provisions	24
Viewing Incident-Linked Amounts	24
Analyzing Incidents	25
Incident Qualitative Analysis	25
<i>Risks and controls</i>	25
<i>Risk factors</i>	26
<i>Risk consequences</i>	26
Incident scope	27
Impact analysis of incidents	28
Managing macro-incidents	28
<i>Connecting incidents to macro-incidents</i>	29
<i>Creating a macro-incident</i>	29
<i>Analyzing macro-incidents</i>	30
Importing and Exporting Incidents	31
Exporting Incidents	32
Importing Incidents	32
Incident Management Process	34
Incident Management Process General Description	34
Incident Management Process Steps	34
<i>Submitting incidents</i>	34
<i>Approving incidents</i>	35
<i>Validating incidents</i>	35
<i>Closing incidents</i>	35
Remediating Incidents	37
Managing Action Plans	38
Creating Action Plans	38
Characterizing Action Plans	38
Action Plan Progress Steps	40
Action Plan Progress Follow-Up	41
Specifying action plan progress rate	41
Using steering calendars	42
<i>Creating a steering calendar</i>	42
<i>Creating steering dates</i>	42
.	43

Managing Actions	44
Creating an Action	44
<i>Action statuses</i>	44
<i>Defining Action Scope</i>	45
Action Management Steps	45
<i>Command proposed to creator</i>	45
<i>Command proposed to entities concerned by an action in "Project" status</i>	45
<i>Command proposed to "Open" action responsible user</i>	45
<i>Commands proposed to the "action plan owner or approver" of a terminated action</i>	46
<hr/>	
Reports HOPEX LDC	47
Incident Analysis Reports	48
Incident and Loss Distribution	48
Incident and Loss Evolution by Month	49
Incident and Loss Evolution by Risk Type	50
Back Testing Reports	51
Back Testing Matrix	51
Back Testing by Risk Type	52
Back Testing by Business Line	52
Capital Calculation Reports	53
Loss Distribution Matrix	53
Basic Indicator Approach (BIA)	54
Standardized Approach (TSA)	54
<hr/>	
Appendix - HOPEX LDC Workflow	57
Incident Workflow	58
Incident Management Workflow Steps	58
Incident Management Workflow Mails	58
<i>Incident approval request</i>	58
<i>Incident modification request</i>	59
<i>Incident validation request</i>	59
Alerts	60
<i>Incident beyond threshold</i>	60
Action Plan Workflow	61



INTRODUCTION



HOPEX LDC integrates different approaches to incident management conforming to Basel II and Solvency II regulations. It helps financial and industrial enterprises to set up effective methodology for management and prevention of incidents.

HOPEX LDC simplifies incident collection and risk quantification using advanced measurement options.

Use of a common repository facilitates sharing of a consolidated vision of risk and encourages promotion of a risk culture within the organization. As an integral part of **HOPEX**, **HOPEX Enterprise Risk Management** and **HOPEX LDC** allow risk managers to access and contribute to information stored in the repository:

The following points are covered in **HOPEX LDC**:

- ✓ "Incident and Loss Administration", page 13
- ✓ "Collecting Incidents", page 17
- ✓ "Remediating Incidents", page 37
- ✓ "Reports HOPEX LDC", page 47
- ✓ "Appendix - HOPEX LDC Workflow", page 57.

For more details on the interface and functions of **HOPEX** in general, see:

- ✓ "The HOPEX Web Front-End desktop", page 31
- ✓ "Defining the Environment for Solutions", page 695

INCIDENT MANAGEMENT PROCESS

Associated with all **HOPEX** Suite products, and more specifically **HOPEX Enterprise Risk Management**, **HOPEX LDC** enables identification, assessment and remediation of incidents.

Declaring incidents

Save time and improve efficiency in incident collection thanks to increased stakeholder involvement, and adapt your risk management methodology to your specific context using the configurable workflow total.

In its standard version, **HOPEX LDC** enables operational participants to easily declare incidents. These incidents are then validated by Risk Managers.

Analyzing incidents

Enhance the incident information repository by adding qualitative and quantitative information. Quantitative information is calculated from losses and gains. These amounts can be specified and calculated in different currencies.

Remediating Incidents

Remediating incidents involves implementation of adequate measures and remediation using action plans and recurrent controls.

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

Obtaining follow-up reports

Guarantee improved consistency of data, reinforce your analysis capacity thanks to advanced report production tools. Encourage communication within your organization for an enhanced enterprise risk culture and improved decision-making. Standard reports are supplied to simplify risk assessment.

CONNECTING TO HOPEX LDC

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

Connecting to the solution

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

Profiles of HOPEX LDC

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

The profiles used are:

- Risk Manager
- Incident and Loss Administrator
- Incident Declarants
- Incident Approvers
- GRC Contributor (Lite)

Presentation of the solution interface depends on the profile selected by the user on connection to the application; the tree of menus and functions varies from one business role to another.

Profiles	Tasks
Incident Declarants or GRC Contributor (Lite)	<ul style="list-style-type: none"> - Create incidents, modify before submission or delete - Analyze incidents (context and losses) - Define and implement action plans <p>➡ As a business user, you may also connect with the "GRC Contributor (Lite) profile". For more details on this profile common to all GRC solutions, see "The GRC Contributor Desktop".</p>
Incident Approvers or GRC Contributor (Lite)	<ul style="list-style-type: none"> - Create incidents, modify before submission or delete - Analyze incidents (context and losses) - Define and implement action plans - Approve a newly-declared incident <p>➡ As a business user, you may also connect with the "GRC Contributor (Lite) profile". For more details on this profile common to all GRC solutions, see "The GRC Contributor Desktop".</p>
Risk Manager and Local Risk Manager	<ul style="list-style-type: none"> - Create, modify and delete incidents - Import a series of incidents by means of an Excel table - Intervene at each step of the incident management workflow: declaration, validation and closing - Analyze incidents (context and losses) - Define and implement action plans - Consult and creates reports.
Incident and Loss Administrator	<ul style="list-style-type: none"> - Have all rights on workflows, objects and menus of the solution - Prepare the work environment and create elements required for management of incidents and losses. - Manage users and assignment of roles - Can intervene on declared incidents, action plans and actions

INTERFACE PRESENTATION

The menus and commands available in **HOPEX LDC** depend on the profile with which you are connected. See ["Profiles of HOPEX LDC", page 7](#).

Incidents and Losses Administrator space

The incident and Losses Administrator has three desktops:

- **Administration** desktop.
- **Environment** desktop, which enables definition of the work environment. See ["Incident and Loss Administration", page 13](#).
- **Incidents** desktop, which presents the tabs corresponding to the main risk management steps:
 - **Home**: enables easy access to the different folders and objects for which the user is responsible
 - **Incidents**: enables access to the list of incidents declared, analyzed or in course of analysis.
 - **Treatment**: enables specification and implementation of action plans and controls designed to treat risks.
 - **Reports**: accesses reports enabling analysis and follow-up of implementation of controls and risks.

Risk Manager space

The Risk Manager has two desktops **Environment** and **Incidents** identical to the desktops of the Incidents and Losses Administrator.

Incident Approver space

The Incident Declarant has only the **Home** tab of the **Incidents** desktop. He/she obtains from this tab the list of incidents to be approved.

Incident Declarant space

The Incident Declarant has only the **Home** tab of the **Incidents** desktop.

ABOUT THIS GUIDE

This guide presents how to make best use of **HOPEX LDC** to assure efficient management of your incidents.


Guide Structure

The **HOPEX LDC** guide comprises the following chapters:

- ["Incident and Loss Administration", page 13](#): describes initializations of reference data to be set up to remediate incidents.
- ["Defining the Environment for Solutions", page 695](#): presents how to describe the environment used in **HOPEX LDC**.
- ["Collecting Incidents", page 17](#): presents functionalities proposed by **HOPEX LDC** to declare and analyze incidents
- ["Remediating Incidents", page 37](#): describes operation of action plans.
- ["Reports HOPEX LDC", page 47](#), presents reports proposed by **HOPEX LDC** to analyse risks;
- ["Appendix - HOPEX LDC Workflow", page 57](#), describes workflows delivered as standard in **HOPEX LDC**.

Additional Resources

This guide is supplemented by:

- The **HOPEX Common Features** guide describes the Web interface and tools specific to **HOPEX** solutions.
 *It can be useful to consult this guide for a general presentation of the interface.*
- the **HOPEX Enterprise Risk Management** guide, which describes functionalities proposed by this **HOPEX** product for risk management.
- The **HOPEX Collaboration Manager** guide for more information on action plans.
- the administration guide **HOPEX Power Supervisor, HOPEX Power Supervisor**, for management of profiles and roles of your users.

Conventions Used in the Guide

Styles and formatting

- 👉 *Remark on the preceding points.*
- 📖 *Definition of terms used.*
- 😊 *A tip that may simplify things.*
- 🐘 *Compatibility with previous versions.*
- 💣 **Things you must not do.**



Very important remark to avoid errors during an operation.

Commands are presented as seen here: **File > Open**.

Names of products and technical modules are presented in bold as seen here:
HOPEX.

INCIDENT AND LOSS ADMINISTRATION



So that the different participants can play their mission, the Incidents and Losses Administrator must first prepare the work environment:

- ✓ Define users and roles
 - See the **HOPEX Administration** guide, chapter "Managing users".
- ✓ Preparing the Work Environment
 - See ["Defining the Environment for Solutions"](#), page 695.
- ✓ ["Preparing Financial Amount Management"](#), page 14.

PREPARING FINANCIAL AMOUNT MANAGEMENT

Administration of information relating to financial amounts includes:

- "Managing Multiple Currencies", page 14
- "Managing Threshold Amounts", page 16

Managing Multiple Currencies

The following points indicate how to manage financial amounts in the local currency of each participant while maintaining a central currency.

➤ For more information on use of multiple currencies in **HOPEX LDC**, see "Recording Incident-Linked Amounts", page 20.

Principle of use

The local currency is the default currency defined for each user of the application. All totals are converted in this currency.

The central currency is the currency adopted by the enterprise as reference currency to consolidate accounts. The amount of an incident, gain or loss is computed in the central currency.

The exchange rate enables calculation, in user currency, of the different amounts associated with incidents in the repository.

Defining Central Currency

The currency that will be used for consolidation of financial amounts should be specified at installation of **HOPEX**.

To define central currency:

1. In the folder where **HOPEX** is installed, launch "Administration.exe" and connect with a user that has data administration authorization rights.

➤ The "System" identifier enables connection with the "Administrator" user. This user is created by default, with repository administration rights. It has no profile (it has all rights) and no password is assigned at installation.

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. In the **Monetary Symbol** field, specify the symbol of your consolidation currency, for example "\$".
6. In the **Central Currency** field, select your consolidation currency, for example "US Dollar".
7. Click **OK**.
8. Exit the Administration application.

Defining Local Currency


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

To define the list of local currencies:

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

Defining user local currency

Local currency of a user is defined at the level of the entity to which the user belongs.

 *By default, an entity inherits the local currency of its parent entity. It is not therefore necessary to define the currency of all entities of the application.*

To define local currency of an entity:

1. Select **Environment > Organization > Entities**.
The tree of entities appears in the edit area.
2. Select the entity that interests you.
The entity properties window appears on the right of the edit area.
3. Select the **Characteristics** tab.
4. Expand the **Characteristics** section and in the **Local Currency** field select the local currency of the entity.

Define exchange rates

By default, amounts concerning incidents are entered in the central currency (defined at installation).

You can however choose to enter an amount in local currency. In this case, it is necessary to first define an exchange rate.

To define an exchange rate:

1. Select **Administration > Currencies > Exchange Rates**.
The list of existing rates appears in the edit area.
2. Click **New**.
3. Select the **Origin Currency Code**.
4. Select the **Final Currency Code**.
5. Enter an exchange **Rate** of the origin currency related to the final currency.
6. Define the period over which the exchange rate is valid by specifying the **Rate Start Date**.

 *The **Rate End Date** is automatically computed by the system.*

7. Click **OK**.
The currencies and their associated exchange rates appear. They are now available for entering values linked to incidents.

Managing Threshold Amounts

To define the threshold amount of losses:

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 **Documentation > Loss Data Collection** folder
The right pane presents data.
5. In the **Net Loss Threshold** field, specify the minimum amount of net losses.
6. In the **Threshold Currency** field, select the currency associated with the threshold amount.
7. Click **OK**.
8. Exit the Administration application.

COLLECTING INCIDENTS



The Incident Data Collection (IDC) module of **HOPEX LDC** allows 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 Risk Manager can then analyze the incident before validating the 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.

- ✓ ["Declaring Incidents", page 18](#)
- ✓ ["Recording Incident-Linked Amounts", page 20](#)
- ✓ ["Analyzing Incidents", page 25](#)
- ✓ ["Incident Management Process", page 34](#)

DECLARING 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.

All profiles are authorized to create incidents.



The Risk Manager may then supplement incident description by recording possible losses.

Creating incidents

To create an incident:

1. Select **Home > My Desktop > New Incident**
Incident properties appear in the edit area.
2. Specify for example its **Name**.
3. Specify the **Declarant Entity**, which is a required field.



An entity can be internal or external to the enterprise: an entity represents an organizational element of enterprise structure such as a management, department, or job function. It is defined at a level depending on the degree of detail to be provided on the organization (see org-unit type). Example: financial management, sales management, marketing department, account manager. An external entity represents an organization that exchanges flows with the enterprise, Example: customer, supplier, government office.

4. Click the **Save** button.

Specifying incident characteristics

To modify characteristics of an incident:

1. Select **Home > My Desktop > My Incidents**
2. The list of incidents you have declared appears in the edit area.
3. Select the incident you want to modify and click **Properties**.
The properties page of the incident appears.
4. Select the **Characteristics** tab.

5. The following information can be specified:
 - **Description** is a comment describing the incident.
 - **Declaration Date, Detection Date** and current **Occurrence Date**, which constitute incident key dates.
 - ☛ To specify a date, use the calendar at the right of the field.
 - ☛ Incident declaration and detection dates can differ, the declaration date being later than the detection date.
 - **Macro-incident**: to connect the current incident to an existing or new Macro-Incident.
 - 📖 A macro-incident is an incident that has consequences on more than one business function or company of the same group.
 - ☛ For more details, see "[Managing macro-incidents](#)", page 28.
 - **Near-miss**: check box to be selected if it is a *near-miss* incident.
 - 📖 A near-miss is an incident that could have caused important financial losses or harm to persons, property or the environment.
 - **Nature**: you may enter the financial nature of the incident.
 - **Status**: Indicates current status of the incident in the incident management process.
 - ☛ The **Status** appears grayed since it is managed by the workflow associated with the incident. For more details, see "[Incident Management Process](#)", page 34.

Duplicating incidents

Only the profiles Risk Manager and Administrator of incidents and losses have this function.

Losses, gains, provisions and recoveries associated with the initial incident are duplicated. Dates are updated relative to the current date.

The incident created must be submitted for validation.

To validate an incident:

1. Select **Home > My Desktop > My Incidents**
The list of incidents you have declared appears in the edit area.
2. Select the objects you want to delete and click **Delete**.
The duplicated incident appears in the list.

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 consequence of an incident.



A gain is the positive financial consequence of an incident.



A provision is an amount deducted from the result to cover incident risks or unexpected charges. Several provisions can concern one and the same risk.



A recovery is a sum, which in certain circumstances can reduce the amount of losses linked to an incident. It enables recovery of a proportion of the amounts involved in the incident.

Accessing Incident Financial Analysis

To access financial analysis data of an incident:

1. Select **Home > My Desktop > My Incidents**
The list of incidents you have declared appears in the edit area.
2. Select the incident you want to modify and click **Properties**.
The properties page of the incident appears.
3. Select the **Financial Analysis** tab.
Total amounts appear in the **Total Amounts** section.




For more details on incident total amounts, see ["Viewing Incident-Linked Amounts"](#), page 24.

Entering a Loss

To enter a *loss*:



A loss is the negative financial consequence of an incident.

1. Access **Financial Analysis** of the incident.
 *For more details, see ["Accessing Incident Financial Analysis"](#), page 20.*
2. Expand the **Losses, Gains, Recoveries and Provisions** section.
3. Select the **Losses** tab and click the **New** button.
The new loss appears in the list.
4. Select the new loss and click **Properties**.
The properties dialog box of the new loss opens.

5. 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 ["Incident and Loss Administration", page 13](#).
6. Click the button at the left of the **Amount** field to select currency of the loss.
 - ☞ 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.
7. 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", page 21](#).
8. 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 ["Defining the Environment for Solutions", page 695](#).
- ☞ For further details on the various configuration possibilities of these characteristics, see ["Incident and Loss Administration", page 13](#).

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 high level classification of main enterprise activities. It corresponds for example to major product segments or to distribution channels. It enables classification of enterprise processes, organizational units or applications that serve a specific product and/or specific market. Regulation frameworks of certain industries impose their own business lines.

- **risk types** to be associated with the loss



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

- **business processes** and **organizational processes** concerned by the loss



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



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

- **products** impacted by the loss



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

- **applications** impacted by the loss



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

- **requirements** expected related to loss management



A requirement is a need or expectation explicitly expressed, imposed as a constraint to be met within the context of a project. This project can be a certification project or an organizational project or an information system project.

Entering Gains



A gain is the positive financial consequence of an incident.

To enter a gain:

1. Access **Financial Analysis** of the incident.




For more details, see "[Accessing Incident Financial Analysis](#)", page 20.

2. Expand the **Losses, Gains, Recoveries and Provisions** section.
3. Select the **Gains** tab and click the **New** button.
The new gain appears in the list.
4. Select the new gain and click **Properties**.
The properties dialog box opens.

5. 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 ["Financial Accounts", page 713](#).
6. 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.
7. 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", page 21](#).
8. Click **OK**.

Recording Recoveries

 A recovery is a sum, which in certain circumstances can reduce the amount of losses linked to an incident. 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. Access **Financial Analysis** of the incident.
 - ☞ For more details, see ["Accessing Incident Financial Analysis", page 20](#).
2. Expand the **Losses, Gains, Recoveries and Provisions** section.
3. Select the **Recoveries** tab and click the **New** button.
The new recovery appears in the list.
4. To specify information specific to a recovery, proceed in the same way as for a gain.
 - ☞ For more details, see ["Entering Gains", page 22](#).

Recording Provisions



A provision is an amount deducted from the result to cover incident risks or unexpected charges. Several provisions can concern one and the same risk.

To enter a **provision**:

1. Access **Financial Analysis** of the incident.



For more details, see ["Accessing Incident Financial Analysis", page 20.](#)

2. Expand the **Losses, Gains, Recoveries and Provisions** section.
3. Select the **Provision** tab and click the **New** button.
The new provision appears in the list.
4. To specify information specific to a provision, proceed in the same way as for a gain.



For more details, see ["Entering Gains", page 22.](#)

Viewing Incident-Linked Amounts

The **Total Amounts** section of the incident properties automatically calculates the sum of all incident-linked financial elements (losses, gains, recoveries and provisions).

If an element is **Estimated**, it is not included in the losses total.

Amounts appear in the central currency and in the local currency.



For more details on currency, see ["Managing Multiple Currencies", page 14.](#)

Total Amounts		
Gross Loss:	0.00 €	Gross Loss (local):
Gross Actual Loss:	0.00 €	Gross Actual Loss (local):
Recoveries:	0.00 €	Recoveries (local):
Net Loss:	0.00 €	Net Loss (local):
Net Actual Loss:	0.00 €	Net Actual Loss (local):

The following fields give valuated indications on incidents:

- **Gross Loss**
Sum of losses related to the incident (including estimated losses). - Gains
- **Gross actual loss**
Gross Actual Loss = Sum of losses related to the incident without estimated losses .- Gains.
- **Recoveries**
Sum of insurance and non-insurance recoveries
- **Net Loss**
Net Loss = Gross Loss - Recoveries
- **Net Actual Loss**
Net Actual Loss = Gross Actual Loss - Recoveries

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 ["Defining the Environment for Solutions"](#), page 695.

☛ For more details on updating these elements in the context specific to incident management, see ["Incident and Loss Administration"](#), page 13.

To complete incident analysis elements:

1. Select **Home > My Desktop > My Incidents**
The list of incidents you have declared appears in the edit area.
2. Select the incident you want to modify and click **Properties**.
The properties page of the incident appears.

Incident Qualitative Analysis

To access incident qualitative analysis:

1. Open the properties of the incident.
2. In the **Characteristics** tab, expand the **Qualitative Analysis** section.

Risks and controls

Associating an incident to a **risk** and to a **control** is an essential step in managing incidents.

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

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

To do this:

1. Open the properties of an incident, **Characteristics** tab, section **Qualitative Analysis**.
2. Click the arrow at the right of the **Risk** field and select **Link Risks**.
The list of risks defined in your repository appears.
3. Select the risk that interests you and click **OK**.
The incident is now attached to the risk.

4. Specify the **Impact** characterizing impact of the incident on environment elements.
 - "Very High"
 - "High"
 - "Medium"
 - "Low"
 - "Very Low"
5. Specify the **Priority** characterizing the incident relative importance.
 - "High"
 - "Medium"
 - "Low"
6. Click the arrow at the right of the **Control** field and select **Link Controls**.
The list of controls defined in your repository appears.
7. Select the control that interests you and click **OK**.
The incident is now attached to the control.

Risk factors

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



A risk factor is an element which contributes to the occurrence of a risk or which triggers a risk. Several risks can originate from the 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 requirement definition, etc.

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. Open the properties of an incident, **Characteristics** tab, section **Qualitative Analysis**.
2. Select the **Risk Factor** tab and click the **Connect** button.
The list of risk factors defined in your repository opens.
3. Select the risk factor associated with the incident.
4. Click **OK**.
The risk factor appears in the list.

Risk consequences



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

To define risk consequences associated with an incident:

1. Open the properties of an incident, **Characteristics** tab, section **Qualitative Analysis**.
2. Select the **Risk Consequence** tab and click the **Connect** button.
The list of risk consequences defined in your repository opens.
3. Select the risk consequences associated with the incident.

4. Click **OK**.
The risk consequence appears in the list.

Incident scope

Incident scope enables definition of risk location within the organization.

☞ Organization description is detailed in paragraph "[Organization](#)", [page 697](#).

☞ For further details on the various configuration possibilities of these characteristics, see "[Incident and Loss Administration](#)", [page 13](#).

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 high level classification of main enterprise activities. It corresponds for example to major product segments or to distribution channels. It enables classification of enterprise processes, organizational units or applications that serve a specific product and/or specific market. Regulation frameworks of certain industries impose their own business lines.

- **risk types** to be associated with the incident

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

- **business processes** and **organizational processes** concerned by the incident

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

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

- **products** impacted by the incident

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

- **applications** impacted by the incident

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

- **requirements** expected related to incident management

📖 A requirement is a need or expectation explicitly expressed, imposed as a constraint to be met within the context of a project. This

project can be a certification project or an organizational project or an information system project.

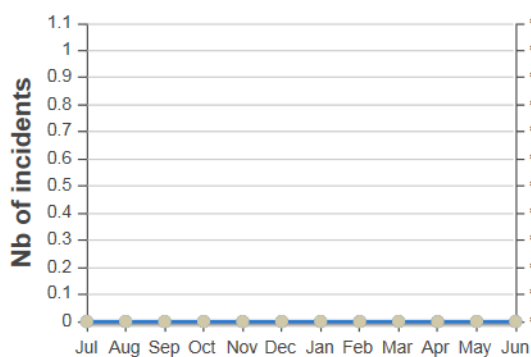
Impact analysis of incidents

In addition to the standard reports presented in chapter "Reports HOPEX LDC", page 47, **HOPEX LDC** offers the possibility of analyzing, from several perspectives, the distribution of incidents linked to a component.

To access the component that interests you, an entity for example:

1. Select **Incidents > Impact Analysis**.
A list of the following folders is proposed.
 - Incidents by process
 - Incidents by entity
 - Incidents by risk type
 - Incidents by business line
 - Incidents by macro-incident.
2. Expand the "Incidents by entity" folder for example.
3. Select the entity that interests you.
Incident properties appear in the edit area.
4. Select the **Reporting > Incidents** tab.
This report presents distribution of net incidents and losses linked to the selected entity on several perspectives: by month, by risk type, by entity, by process and by business line.

Incidents and net loss per month



Scale of the number of incidents is presented on the left, and scale of loss amounts is presented on the right.

Managing macro-incidents

An incident concerns only one business line and one organizational unit, which is why **HOPEX LDC** 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 incident that has consequences on more than one business function or company of the same group.

For example, a wilful incident in a building can have repercussions on several business lines or organizational units of the group.

Connecting incidents to macro-incidents

You can connect incidents to macro-incidents in two ways:

- from the properties of a macro-incident, in the **Incidents** tab, by connecting existing incidents
- from an incident (operation described below)

To connect an incident to the macro-incident:

1. Select **Home > My Desktop > My Incidents**
The list of incidents you have declared appears in the edit area.
2. Select the incident you want to modify and click **Properties**.
The properties page of the incident appears.
3. Select the **Characteristics** tab.
4. Click the arrow at the right of the **Macro-Incident** field and select **Link Macro Incidents**.
The list of macro-incidents appears.
5. Select the macro-incident that interests you and click **OK**.
The incident is now attached to the macro-incident.

➤ Incidents are visible in the **Incidents** tab of the macro-incident.

Creating a macro-incident

➤ This feature is proposed only to Risk Managers and Incidents and Losses Administrators.

You can create macro-incidents in two ways:

- from an incident, an operation similar to that described above:
["Connecting incidents to macro-incidents", page 29](#)
- from the **Incident Management** tab (operation described below).

To create a macro incident:

1. Select **Incidents > Incident Management > Macro-Incidents**.
The list of macro-incidents you have declared appears in the edit area.
2. Click **New**.
The new macro-incident appears in the list.
3. Select the macro-incident that interests you and click **Properties**.
The properties page of the macro-incident opens.
4. In the **Characteristics** tab, complete 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](#)", page 21.

Analyzing macro-incidents

Incidents connected to the macro-incident

To access the list of incidents connected to a macro-incident:

1. Open the properties of the macro-incident and select the **Incidents** tab.

☛ In the **Characteristics** tab of the macro-incident, the fields **Number of Validated Incidents**, **Date of First Occurrence** and **Date of Last Occurrence** are completed automatically.

Macro-incident amounts

The **Total Amounts** section of the macro-incident properties presents the sum of all financial elements specified for incidents connected to the macro-incident.

The following fields are calculated automatically:

- **Gross Loss**
Sum of losses related to the incident (including estimated losses).- Gains
- **Gross actual loss**
 $\text{Gross Actual Loss} = \text{Sum of losses related to the incident without estimated losses} - \text{Gains}$.
- **Recoveries**
Sum of insurance and non-insurance recoveries
- **Net Loss**
 $\text{Net Loss} = \text{Gross Loss} - \text{Recoveries}$
- **Net Actual Loss**
 $\text{Net Actual Loss} = \text{Gross Actual Loss} - \text{Recoveries}$

Losses evolution report

This report presents evolution of net losses per month of incidents connected to the macro-incident.

IMPORTING AND EXPORTING INCIDENTS

HOPEX LDC Use Excel data exchange wizards to import and export incidents.

For more details, see chapter "Excel Import/Export Wizards" in the **HOPEX Common Features** guide.

The list of information exported in the standard model delivered with **HOPEX LDC** is as follows:

- Incident **Name**
- **Description** is a comment describing the incident
- **Declarant**: name of the incident creator
- **Declarant entity**:
- **Declaration date**
- **Detection date**
- **Occurrence date**
- **Near-miss**:



A near-miss is an incident that could have caused important financial losses or harm to persons, property or the environment.

- **Nature**: you may enter the financial nature of the incident.
- **Impact** of the incident on environment elements
- **Priority** characterizing described incident relative importance
- **Currency**
- **Gross loss** is obtained by a macro
- **Recoveries** is obtained by a macro
- **Provision**: the amount is obtained by a macro.
- **entity** 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 high level classification of main enterprise activities. It corresponds for example to major product segments or to distribution channels. It enables classification of enterprise processes, organizational units or applications that serve a specific product and/or specific market. Regulation frameworks of certain industries impose their own business lines.

- **risk types** to be associated with the incident



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

- **business processes** and **organizational processes** concerned by the incident



A business process represents a system that offers products or services to an internal or external client of the company or organization. At the higher levels, a business process represents a structure and a categorization of the business. It can be broken down into other

processes. The link with organizational processes will describe the real implementation of the business process in the organization. A business process can also be detailed by a functional view.



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

- **products** impacted by the incident



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

- **applications** impacted by the incident



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

- **requirements** expected related to incident management



A requirement is a need or expectation explicitly expressed, imposed as a constraint to be met within the context of a project. This project can be a certification project or an organizational project or an information system project.

Exporting Incidents



To be able to use Excel Export from a listview: open the user options window, select the folder **Data Exchange > Import/Export synchronization > Tools/Third Party Formats** and check that the **Excel Export: Availability in Listviews** option is selected.

To run the wizard for export of **HOPEX LDC** data to an Excel file:

1. Select **Incidents > Incident Management > Excel > Export**.
2. Note that the **Predefined Template File** is "Incident Template".
3. In the **Excel Export File** field, select the type of file you want to generate (xls or xlsx).


To run the wizard for export of **HOPEX LDC** data to an Excel file:

1. Access the list of incidents you want to export, for example select **Incidents > Incident Management > Closed Incidents**.
The list of closed incidents appears in the edit area.
2. Right-click the incidents you want to export.
3. Click **Excel** to start export.
The file opens in an xls table. You can save it if you wish.

Importing Incidents

To import incidents from an Excel file in **HOPEX LDC**:

1. In HOPEX, select **Incidents > Incident Management > Excel > Import**.
The import wizard appears in the edit window.
2. At the right of the **Excel Import File** field, click the **Browse** button.
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. So that imported data will be visible in **HOPEX**, click **Finish**.
8. To modify import parameters, click **Previous**.
9. To discard import, click **Cancel**.

INCIDENT MANAGEMENT PROCESS

Incident Management Process General Description

☛ For more information on action plan workflow, see ["Action Plan Workflow", page 61.](#)

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 a notification by mail and the new incident appears with status "Submitted".
- When an incident has been submitted by its declarant,, the incident approver can:
 - **Approve** the incident which takes status "To Be Validated".
A notification is sent by mail to the Risk Manager.
 - **Request modifications** of the incident which takes status "Project".
A notification is sent by mail to the incident declarant.
 - **Reject** the incident.
In this case, the incident takes status "Rejected", but is not destroyed.
- When an incident has "to be validated" status, 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".

Incident Management Process Steps

Submitting incidents

When you have specified information concerning the incident, you can submit it to the Incident Approver.

To submit an incident:

1. Select **Home > My Desktop > My Incidents**
The list if incidents you have declared appears in the edit area.

2. Right-click the incident you want to submit and select **Incident Declaration To Be Submitted**.
 - If the incident declarant has role "Incident Declarant", the incident takes status "To Be Approved" and appears in the list of incidents to be approved by the Incident Approver.
 - 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.

Approving incidents

This step is only proposed if the incident declarant has role "Incident Declarant" and the incident has taken status "To Be Approved".

To approve an incident:

1. Select **Home > My Desktop > My Incidents to Approve**
The list if incidents you have to approve appears in the edit area.
2. Right-click the incident that interests you and select one of the following commands:
 - **Approve** the incident which takes status "To Be Validated".
A notification is sent by mail to the Risk Manager.
 - **Request modifications** of the incident which takes status "Project".
A notification is sent by mail to the incident declarant.
 - **Reject** the incident.

Validating incidents

When incidents have been specified with their losses, recoveries and provisions, you can then make use of your data. Only Risk Managers are authorized to validate incidents.

To validate an incident:

1. Select **Home > My Desktop > My Incidents**
The list if incidents for which you are responsible appears in the edit area.
2. Right-click the incident that interests you and select one of the following commands:
 - **Validate** the incident, which takes status "Validated".
 - **Reject** the incident.

Closing incidents

When the incident has been validated, the Risk Manager can decide that this incident will not be modified further, and therefore close it .

To do this:


1. Select **Home > My Desktop > My Incidents**
The list if incidents for which you are responsible appears in the edit area.
2. Right-click the incident you want to close and select **Close**.
The incident then appears in the list of incidents accessible from **Incidents > Incidents > Closed Incidents**.

REMEDIATING INCIDENTS



It is particularly important to identify causes and consequences of incidents to improve risk Management.

HOPEX LDC allows you to specify, implement and follow up *action plans* defined for remediating causes and consequences of incidents.

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

The following points are covered here:

- ✓ ["Managing Action Plans", page 38](#)
- ✓ ["Managing Actions", page 44](#)

MANAGING ACTION PLANS

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



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

Creating Action Plans

To create an action plan from an incident:

1. Open the properties page of an incident and select the **Remediation** tab.
2. In the **Action Plans** section, click the **New** button.
The new action plan is created in the list of action plans of the incident.
The action plan is created with status "Open".

Characterizing Action Plans



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

To update fields that characterize an action plan:

1. Open the properties of the action plan that interests you.
In the **Characteristics** tab, the following sections appear:
 - "General characteristics", page 39
 - "Action plan statuses", page 39
 - "Financial assertion", page 39
 - "Success factors", page 40
 - "Scope", page 40
 - "Milestones", page 40
 - "Attachments", page 40

General characteristics

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

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

Action plan statuses

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

Financial assertion

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

Success factors

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

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

Scope

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

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

Milestones

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

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

Attachments

You can attach business documents to an action plan:

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

Action Plan Progress Steps

Creating the action plan

When the action plan is created, it is in "To submit" state.

By default, the action plan creator is the action plan **Owner**. Having specified the characteristics of a new action plan, the creator can:

- **Propose** the action plan.
In this case, the user defined as "Approver" receives a notification mail, and the new action plan appears with status "To Begin" in his/her tasks list.

Preparing the action plan

The action plan "Responsible" user can **Validate** or **Cancel** the action plan.

- **Validate:** the action plan, which then takes status "In Progress". Actions can then be created.
- **Cancel:** the action plan which takes status "Canceled".

Executing the action plan

Having executed actions relating to the action plan, the "Owner" can:

- **Terminate** the action plan which takes status "Closed". To do this, all action plan actions must be terminated. The "Approver" user is notified of the action plan termination request.

Closing the action plan

After having consulted action plan follow-up reports, the "Approver" user can **Close** and then **Reopen** the action plan.

- **Close**: the action plan, which retains "Closed" status and disappears from the task lists of creator, approver and owner.
- **Reopen**: additional actions can then be created. The action plan again takes status "In Progress".

☛ For more information on action plan workflow, see ["Action Plan Workflow"](#), page 61.

Action Plan Progress Follow-Up

Action plan progress is specified at periodic dates by the action plan responsible user. For more details, see ["Specifying action plan progress rate"](#), page 41.

HOPEX LDC offers the opportunity to regularly remind the action plan responsible user that he must update the progress of his action plan using a steering calendar. So that a reminder e-mail can be automatically sent to the action plan responsible user, you can connect a **Steering Calendar** to the action plan. For more details, see ["Using steering calendars"](#), page 42.

Specifying action plan progress rate

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

To indicate progress of an action plan:

1. Open the properties of the action plan and expand the **Action Plan Progress** section.
2. In the **Progress Rate** table, click **New**. The **Progress Rate** creation page appears.
3. Specify the **Name** of the progress rate.
4. Specify the **Updated Progress Percentage** and add a percentage **Comment**, if required.

5. Verify the **Progress Date**.
6. Specify the **Progress Assessment**:
 - Delayed
 - On Time
7. In the progress rate properties page, click **OK**.
The progress rate appears in the list.
The **Last Progress Percentage** and **Last Progress Percentage Comment** fields are updated.

Using steering calendars

Creating a steering calendar

You can connect a **Steering Calendar** to the action plan so that the action plan responsible user can indicate a progress percentage at dates defined in this calendar. A message is sent to the user on these dates.

 For more details on managing steering calendars, see the technical article **HOPEX Power Studio - Steering calendar**.

To create a steering calendar for an action plan:

1. Open the properties of an action plan.
2. In the **Characteristics** section, click the arrow at the right of the **Steering Calendar** field.
3. Select **Create a steering calendar**.
The steering calendar creation page appears.
4. Specify the **Name** of the steering calendar.
5. In the **Steering Calendar Type** field, leave the default value "Action Plan".
6. In the **Scheduler Configuration** field, leave the default value "Steering Calendar - Configuration scheduler".
7. In the **Reminder** field, leave the default value "Steering Calendar - Emailing SchedulerJob".
8. Click **OK**.
You must then create Steering Dates.

Creating steering dates



A steering date is a date defined in a steering calendar on which a reminder will be sent to the person responsible for an element. This can be an initial date, reminder date or final due date.

To create a steering date for an existing steering calendar:

1. Open the properties of the steering calendar that interests you.

2. In the **Steering Date** section, click **New**.
The new steering date appears in the list.

To define steering date characteristics:

1. Open the steering date properties dialog box and select the **Characteristics** tab.
2. Specify the **Name** of the date, to enable its reuse in another steering calendar if required.
3. Specify the **Date Type**.
 - "Initial" - to signify start of an action plan
 - "Remind" - to remind the responsible user of progress rate update
 - "Last" - to signify close of an action plan
4. Specify messages that will be addressed as notification and as E_mail.
You must then plan the dates of actions execution.

To schedule a steering date:

1. Open the steering date properties dialog box and select the **Scheduling** tab.
You must define the **Start date** (absolute ou Relative) and the **Recurrence Type**.
 - ☛ The start hour is defined in **UTC** format.
 - The **Start date** may be specified by **Start date (absolute)** or by **Relative Date**.
 - ☛ The **Relative Date** is defined related to the **Effective Begin Date** of the action plan.
 - The **Recurrence Type** defines the frequency at which reminders are sent: daily, weekly, monthly, once only.
 - ☛ For details on scheduler configuration, see "Scheduling" chapter in the **HOPEX Power Studio - Steering calendar** technical article

MANAGING ACTIONS



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




The action plan Responsible User must define actions enabling execution of the action plan. The Responsible User can create actions and assign these.

Creating an Action

To create an action from an action plan:

1. Select **Home > My Desktop > My Responsibilities > My Action Plans**.
2. In the page that appears, select the action plan that interests you and click **Property**.
3. In the **Actions** section, click **New**.
The action appears in the list of action plan actions.
4. Open the properties of the action and specify its **Name**.
5. Specify the following fields:
 - **Priority**: enables indication of a level. Priority can be: "Low", "Medium", "High" or "Critical".
 - **Action Responsible**: responsible for the action as specified by the action plan creator.
 - **Owner Entity**: owner organization unit enabling restriction of the list of action owners.
6. You can specify milestones, which are important dates of the action.
 - **Effective Begin Date** and **Planned Begin Date**.
 - **Effective End Date** and **Planned End Date**.
7. Click **OK**.
The action is created with "Created" status.
8. Connect the controls you want to implement.

 *These fields are accessible when the action has taken "Open" status.*

Action statuses

- **Created**: the action is created.
- **Project**: the created action awaits opening by the "action owner".
- **In Progress**: action is accepted by its owner.
- **To Close**: the action is completed and must be approved by the "action plan owner or approver".
- **Closed**: the action is completed and approved.

Defining Action Scope

An action can concern one or several objects of control, risk or application type.

For example, to define the controls that will be executed in the framework of the action:

1. Open the properties of the action.
2. Expand the **Scope** section.
3. Connect the controls you want to implement.

☛ *These fields are accessible when the action has taken "Open" status.*

Action Management Steps

☛ *For more details on an action workflow, see the, chapter "Action Workflow" in the **HOPEX Collaboration Manager guide**.*

When an action has been created, the action creator can declare the action as being in "Project" status.

When all actions of an action plan have been published and accepted, the action plan can be implemented.

Command proposed to creator

Having specified the characteristics of a new action, the "action plan owner or approver" can use the command:

- **Project.**
In this case the user defined as "Responsible User" receives a notification by mail and the new action takes status "Project".

Command proposed to entities concerned by an action in "Project" status

When an action has been proposed by the user the "action plan owner or approver" and the "Responsible" user can:

- **Open** the action, which takes status "Open".

Command proposed to "Open" action responsible user

Having studied action execution possibilities, the "Responsible User" can:

- **Terminate** the action.
A notification is sent to the user defined as "action plan owner or approver".

Commands proposed to the "action plan owner or approver" of a terminated action

After studying characteristics of the action he/she created, the action plan owner or approver" creator can:

- **Close.**
In this case the user defined as "Responsible" receives a notification and the action takes status "Closed".
- **Return to responsible user,** for supplementary actions.

REPORTS HOPEX LDC



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.*

Impact analysis reports are proposed as standard by **HOPEX LDC**, for more details, see ["Impact analysis of incidents", page 28](#). In addition, the following points are covered here:

- ✓ ["Incident Analysis Reports", page 48](#).
- ✓ ["Back Testing Reports", page 51](#).
- ✓ ["Capital Calculation Reports", page 53](#).

INCIDENT 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", page 21](#).

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 process	Business process	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", page 20](#).

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 process	Business process	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 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", page 20](#).

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 process	Business process	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 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", page 21](#).

Risks displayed in reports are the risks defined in parameters and their sub-risks.

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 process	Business process	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

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.

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.

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Net loss threshold	Real	Minimum amount of displayed losses.
Analysis year	Short	Year preceding current year by default.
Risk type	Risk type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Basic Indicator Approach (BIA)

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
- 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).

Report parameters

This consists of selecting incidents and losses that will be presented in specifying elements that define their scope. In this report, the scope is defined by a single business line.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Gross revenue threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Average period	Short	Number of years to which average calculation relates.
Percentage of BIA	Real	Percentage value to be applied.
Business line	Business line	Mandatory.

Standardized Approach (TSA)

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).

Report parameters

This consists of selecting incidents and losses that will be presented by specifying elements that define their scope: risk types, entities, processes or business lines.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Gross revenue threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Average period	Short	Number of years to which average calculation relates.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

APPENDIX - HOPEX LDC WORKFLOW



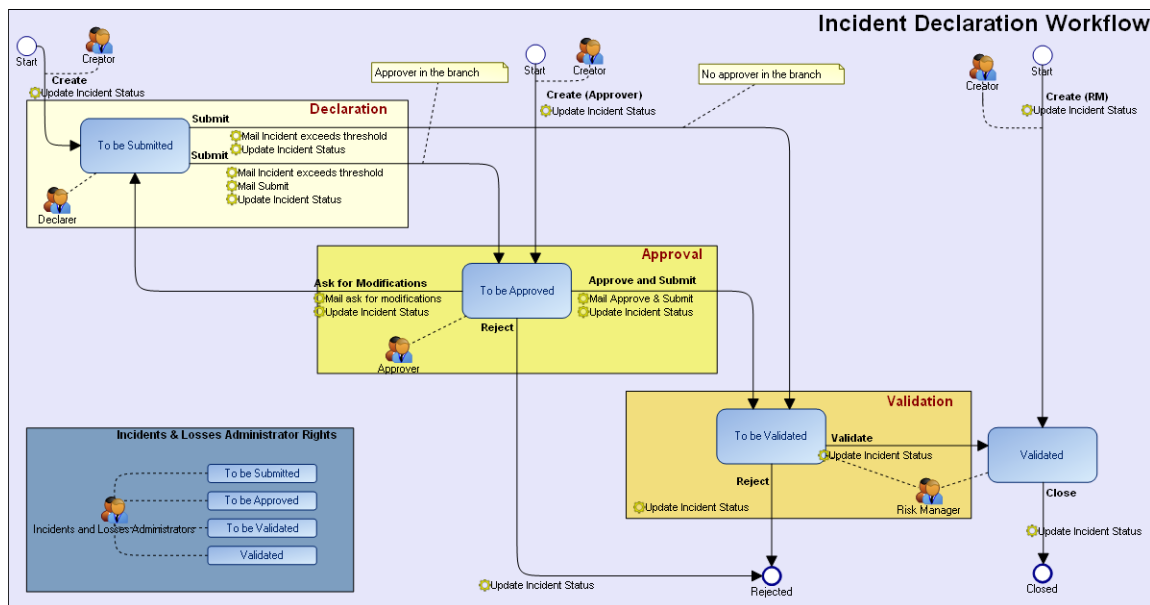
This chapter presents **HOPEX LDC** workflow diagrams.

- ✓ ["Incident Workflow", page 58](#)
- ✓ ["Action Plan Workflow", page 61](#)

INCIDENT WORKFLOW

Incident Management Workflow Steps

Steps in the incident management process are described in "Incident Management Process", page 34.



Incident Management Workflow Mails

Incident approval request

From	Incident Declarant
To	Incident Approver
Subject	Incident to be approved - [Incident Name]
Content	<p>Dear [Approver Name]</p> <p>Please approve the incident [Incident Name]. To enter the application and perform your task, click here.</p> <p>This e-mail has been sent automatically by HOPEX.</p>

Incident modification request

From	Incident Approver
To	Incident Declarant
Subject	Incident to be modified - [Incident Name]
Content	<p>Dear [Declarant Name] [Approver Name] has asked for modifications on the incident [Incident Name] To enter the application and perform your task, click here.</p> <p>Sincerely, Risk Management Team This e-mail has been sent automatically by HOPEX.</p>

Incident validation request

From	Incident Approver
To	Risk Manager
Subject	Incident to be validated [Incident Code] [Incident Name]
Content	<p>Please validate the incident [Incident Code] [Incident Name] To enter the application and perform your task, click here.</p> <p>This e-mail has been sent automatically by HOPEX.</p>

Alerts

Incident beyond threshold

To	Incident Declarant
Subject	alert: High loss declared
Content	<p>An incident with high net loss has been submitted. Incident [Incident Code] [Incident Name] To enter the application and perform your task, click here.</p> <p>This e-mail has been sent automatically by HOPEX.</p>

ACTION PLAN WORKFLOW

Steps in the action plan management process are described in "Action Plan Progress Steps", page 40.

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

The workflow diagram introduces:

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

Action plan workflow

