HOPEX Risk Mapper

User Guide

HOPEX V2

1st Edition (July 2016)

INTRODUCTION

Managing risks, assuring and maintaining compliance with new regulations provides a real opportunity for those managing enterprise changes. In this perspective, **HOPEX Risk Mapper** offers total visibility of operational risks, control points and value chains.

The **HOPEX** repository covers all enterprise resources, from global value chains to IT resources. The **HOPEX Risk Mapper** approach enables business and IT managers to guarantee traceability of compliance controls via application layers, data and infrastructures.

With **HOPEX Risk Mapper**, it is easier to integrate the risk management policy and the compliance controls for corporate governance by, on the one hand, setting realistic goals, and on the other hand, by supplying the deliverables and information required by all the org-units involved.

RISK MANAGEMENT PROCESS

Associated with the all the products in the **HOPEX** suite, **HOPEX Risk Mapper** is used to model the environment, assess the risks to mitigate them and last but not least, to control them with an efficient control policy.

The process recommended by **HOPEX** therefore comprises the following steps:

- *"Modeling the environment", page 2,*
- *"Identifying, analyzing and assessing risks", page 2,*
- *"Remediating Risks", page 3,*
- *"Risk Control Monitoring and Policy", page 3.*

Modeling the environment

Risks must be managed in the external and internal environments of the organization, its strategic objectives and the specific objectives of the risk management activity.

- The external environment defines the external environment in which the organization operates as well as its relationships with this environment.

  ☛ *For more details, see "External Environment", page 18.*

- The internal environment describes the organization. This ensures that risk management acknowledges the major objectives and constraints of the organization.

  ☛ *For more details, see "Internal Environment", page 14.*

- The risk management context is essentially linked to the objectives that the enterprise pursues through its risk management process.

  ☛ *For more details, see "Risk Management Context", page 24.*

Identifying, analyzing and assessing risks

It is necessary to identify the risks concerned, then analyze and assess them to get the elements required for their treatment.

Identifies risks

It is necessary to determine where, when, why and how events might prevent, degrade, delay or improve the achievement of the organization's objectives.

Internal and external events affecting the achievement of entity objectives must be described with the distinction made between risks and opportunities. The opportunities can then be used to form management strategy or in objective-setting processes.

More specifically, several risk identification methods can be proposed depending on the context:

- Method based on organization objectives achievement
- Method based on lists of risk types, risk factors or controls applied to an appearance context
- Method based on historical data (databases of incidents, claims, faults, etc.)

☛ *For more details, see "Identifies risks", page 31.*

Analyzing Risks

This consists of completing the identification of each risk by precisely indicating what could occur, where, when, why, and how this could have arisen. This analysis could reveal new risks that were not directly identified in the previous step. The effectiveness of existing controls that could prevent this risk are also assessed.

☛ *For more details, see "Risk Analysis", page 37.*

Assessing Risks

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

Risks are assessed taking into account:

- their occurrence frequency
- their impact

☛ *For more details, see "Assessing Risks", page 40.*

Remediating Risks

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

The acceptable level for each risk is defined based on previous evaluations.

☛ *For more details, see "Risk Treatment", page 44.*

Remediating risks involves:

- identification of the various options possible
- assessment of these options
- preparation and implementation of remediation plans:
  - *"Implementing Action Plans", page 47*
  - *"Controls", page 48*

Risk Control Monitoring and Policy

Policies and procedures are established and implemented to help ensure that risk responses are effectively carried out.

Monitoring is accomplished through ongoing management activities or independent assessments, or both.

The topics covered in this guide are:
- "Control System Ongoing Improvement", page 56.
- "Control Effectiveness Assessment", page 57.
- "Incident and Loss Monitoring", page 58.

Information and communication

Relevant information is identified, collected, and communicated in a form and timeframe that enable collaborators to carry out their responsibilities. Effective communication should also occur in a broader sense, flowing downwards, across, and upwards in the entity.

Communication and consultation are important considerations at each step of the risk management process. They should involve dialog with stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision-maker to other stakeholders.

☛ *For more information on the functionalities offered by* **HOPEX**, *see* **HOPEX Common Features**, *which describes the tools specific to* **HOPEX** *solutions.*

CONNECTING TO HOPEX RISK MAPPER

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

Connecting to the solution

To connect to **HOPEX Risk Mapper**, see HOPEX Common Features, "HOPEX Web Front-End Desktop".

Managing Options Relating to Risks

The functionalities described in this guide are based on new risk management facilities implemented in the **HOPEX V2** version of **HOPEX**.

Compatibility options are, however, available to transfer your data from one version to another or to continue to work with the functionalities offered by **HOPEX Control and Risk**, for example.

To access the risk management functionalities offered in the **HOPEX** versions prior to version **HOPEX V2** :

1. Open the options window.
2. In the left pane of the options window, expand the **Compatibility** folder then double-click the **Others** folder.
3. In the right part, select the **Risk Compatibility Properties (MEGA 2009)** option.

This option is used, for example, to show the tabs that include **Analyze**, **Situation** or **Redundancy** in the risk properties pane.

By default, only the risk management facilities implemented in the **HOPEX V2** version of **HOPEX** are offered. You can continue to use the facilities and the presentation of **HOPEX** versions prior to this version.

To activate the compatibility option:

1. In the workspace, open the **Options** window.
2. Double-click the **Business Process and Architecture Modeling** icon.
3. Select the **Risk Compatibility Properties HOPEX** option.

☺ *See " CRK to ERM ICM Risk Mapper Data Migration Toolkit " technical artical, " technical articles " chapter. This article presents the migration tools from **MEGA Control and Risk** ormat **HOPEX Risk Mapper** / **HOPEX Enterprise Risk Management** format.*

Profiles of HOPEX Risk Mapper

In **HOPEX Risk Mapper**, there are default user profiles with which specific rights and accesses are associated.

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 available are:
- Control and Risk Architect
- Risk Manager (simplified).

Profiles	Tasks
Controls and Risks Architect	The Control and Risk Architect works with the modeling tools offered by **HOPEX**. The Control and Risk Architect is responsible for identifying and assessing risks within the scope for which the Control and Risk Architect is responsible. - Risk identification - Direct assessment - Creating analysis reports.
Risk Manager (simplified).	The Risk Manager (simplified) has access to a solution offered by **HOPEX Solutions**. The Control and Risk Architect is responsible for identifying and assessing risk within the scope for which the Control and Risk Architect is responsible, but does not have access to all the **HOPEX** modeling facilities. For example, the Control and Risk Architect cannot use diagrams.

INTERFACE PRESENTATION

The menus and commands available in **HOPEX Risk Mapper** depend on the profile with which you are connected.
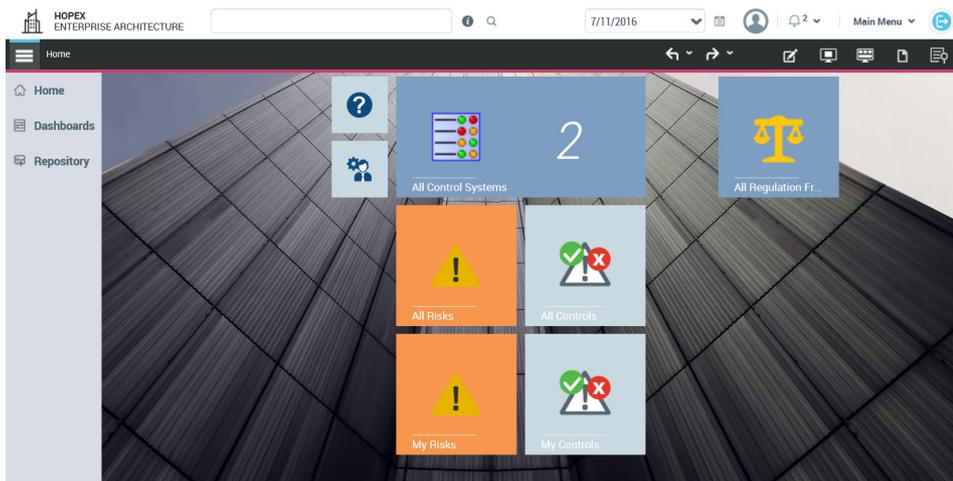
☛ *For more details on how to use the interface, see the **HOPEX Common Features** guide.*

☛

Controls and Risk Architect desktop

The Control & Risk architect has a modeling desktop that contains the objects for which the Control and Risk Architect is responsible.

☛ *For more details, see "Profiles of HOPEX Risk Mapper", page 6.*

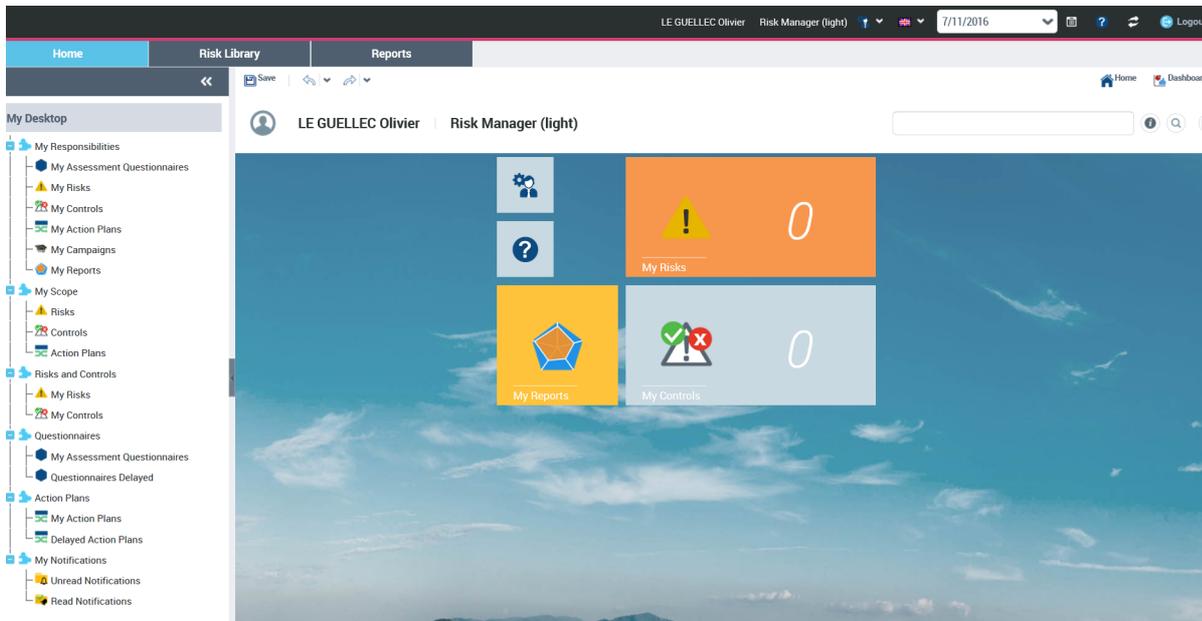The Controls and Risks Architect desktop offers the following paints:

- **Home** : enables easy access to the different folders and objects for which the user is responsible using the following tiles:
  - **All control systems**,
  - **All regulation frameworks**,
  - **All risks** and **my risks**,
  - **All controls**and **my controls**,
- **Repository**: enables access to the list of risks and controls.
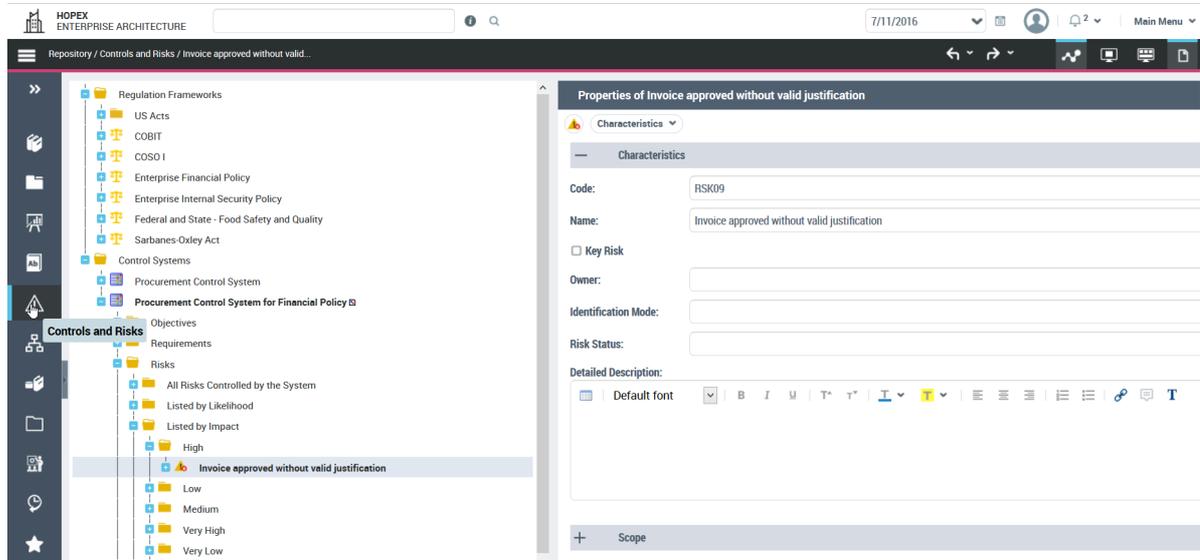
Risk Manager space (simplified)

☛ *For more details on the Risk Manager (simplified) business role, see "Profiles of HOPEX Risk Mapper", page 6.*

The Risk Manager (light) has a risk management desktop with the following tabs:

- **Home** : enables easy access to the different folders and objects for which the user is responsible using the following tiles:
  - **My risks**,
  - **My controls**,
  - **My reports**.
- **Repository**: enables access to the list of risks and controls. Direct assessments can be made from this tab
- **Reports**: accesses reports enabling analysis and follow-up of implementation of controls and risks.

ABOUT THIS GUIDE

This guide presents how to make best use of **HOPEX Risk Mapper** to ensure effective management of your risks.

Guide Structure

The structure of the **HOPEX Risk Mapper** guide is linked to the methodology recommended by **HOPEX**. The guide therefore comprises the following chapters:

- "Environment Analysis", page 13 explains how to describe, with **HOPEX Risk Mapper,** the internal and external and internal environments of your organization as well as the context of your risk management project
- "Assesses risks", page 29: presents functionalities proposed by **HOPEX Risk Mapper** to declare and analyze incidents
- "Risk Treatment and Controls", page 43: presents functionalities proposed by **HOPEX Risk Mapper** to declare and analyze incidents
- "Risk Control Policies Operational Monitoring", page 55, describes how to use and maintain objects implemented within the framework of the risk management policy
- "Reports HOPEX Risk Mapper", page 59, presents reports proposed by **HOPEX Risk Mapper** to analyse risks;

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 Business Process Analysis** guide, which describes the functionalities offered for risk management,
- the **HOPEX Enterprise Risk Management** guide, which describes functionalities proposed for risk management.
- The **HOPEX LDC** guide, which describes the functionalities offered 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**.

ENVIRONMENT ANALYSIS

Analysis of the environment in which the risk management project will be carried out enables definition of basic parameters according to which risks must be managed, with an indication of project scope. This analysis includes the internal and external environments of the organization, its strategic objectives and the specific objectives of the risk management activity.

This chapter presents how to describe a risk management project environment with **HOPEX Risk Mapper**.

This chapter explains how to describe and analyze, with **HOPEX Risk Mapper**, the following elements:

INTERNAL ENVIRONMENT

The internal environment includes the culture and spirit of the organization. It sets the basis for how risk is viewed and addressed by all entity co-workers, particularly risk management philosophy and risk appetite, integrity and ethical values, and the environment in which the organization operates.

At this stage it is possible to take an inventory of:

- the list of strategic *objectives* of the organization and the associated *requirements*
  Objectives must exist before management can identify the events that may affect their achievement. Risk management ensures that objectives are in line with the mission of the organization and its risk appetite.

- What exists in the enterprise (organizational chart, *processes*, *management rules*, *,control systems*, responsibilities, *applications*, *infrastructures*)

Defining the internal environment ensures that risk management acknowledges the major objectives of the organization.

Organization of internal org-units

The different org-units concerned must be involved at each step of the risk management project via a communication and consultation process.

This enables building a solution that will be better accepted by the different stakeholders.

To access all entities of the organization with the **Control and Risk Architect** business profile:

❭ From the **Repository** paint, select **Main Objects**, then unfold the**Org-Units** folder.
  The list of all org-units appears.

To define the list of *org-units* concerned, **HOPEX Risk Mapper** enables you to enter the enterprise organizational chart.

To do this, from an org-unit,select **New > Org-Unit Org Chart**.
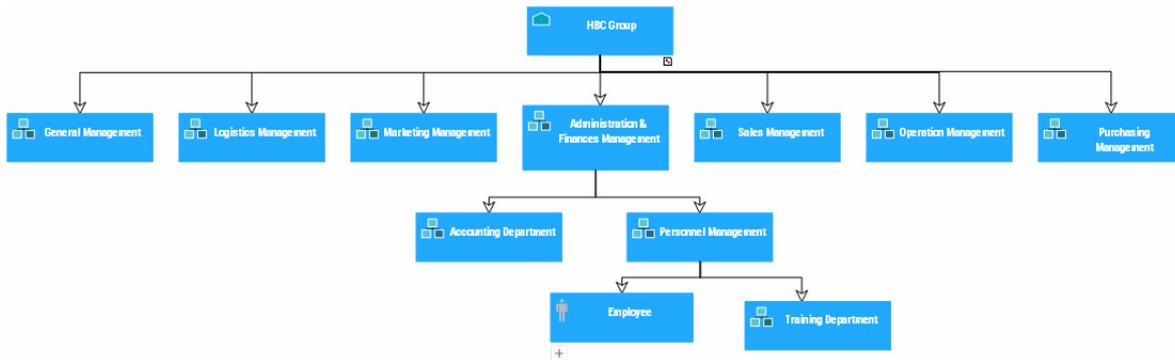
Enterprise hierarchical and functional organizational chart

☛ *For more information on organizational charts, see "Organizational Chart and Responsibilities" in **HOPEX Business Process Analysis***

☛ *To access all entities of the organization with the **Risk Manager (simplified)** business profile: in the **Risk Library** tab, select **Risk Tree** and expand the **Risks by Entity** folder.*

You can also define objectives and requirements for each organization unit.

Organization objectives and requirements

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

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

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

With **HOPEX Risk Mapper**, the objectives and requirements of your organization are defined in the properties of the org-unit that represents the organization.

To define the *objectives* and *requirements* of each org-unit:
1. Open the properties of the org-unit.

2. Select the **Objectives and requirements** tab.
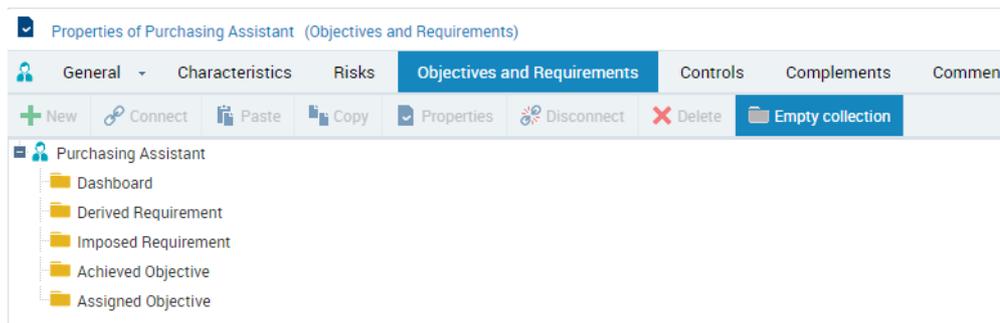
Here you can create new objectives and requirements or connect those which already exist.

☞ *For more information on the definition of objectives and requirements, see "Objectives and Requirements" in* ***HOPEX Common Features***.

Organization Processes

To access the   business processes with the ***Control and Risk Architect*** profile:

❱ From the **Repository** paint, select **Main Objects**, then unfold the**Business Process** folder.
If you expand the folder of a process, you can display the sub-processes owned by the current process.

☞ *To access all processes in the repository with the **Risk Manager (simplified)** profile: in the **Risk Library** tab, select**Risk Tree > Risk by Process.***

Process types

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.*

- Functional process

  📖 *A functional process is a value chain providing results as goods or services, to an internal or external client of the enterprise or organization. This value chain is described as a sequence of activities.*

The types are distinguished by different icons in the trees and lists.

The tabs in the properties dialog box of a business process:

The properties window of a process presents the following sections:
- **Characteristics**: to present the persons responsible for the process. For more details, see "RACI on a risk", page 35.
- **Risks**: lists the risk that relate to the process. For more details, see "Assesses risks", page 29.
- **Objectives and Requirements**: for more details, see "Organization objectives and requirements", page 15.
- **Comments** : for a text of the process.

Applications

The description of the internal context in which the risk management process operates can be supplemented by the description of the IT *applications* concerned.

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

To access applications with the ***Control and Risk Architect*** profile:
1. From the **Repository** paint, select **Main Objects**.
2. Expand the **Applications** folder.
   The list of applications defined in the database appears.
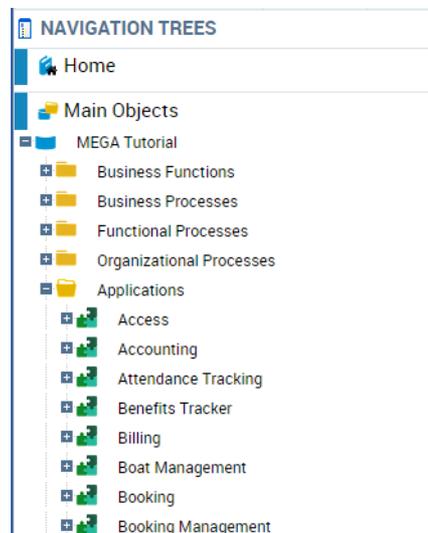
You can associate *objectives* and *requirements* with each application.

    ☞ *If you have the **HOPEX IT Architecture** product, you can also describe application operation as a sequence of sub-applications or services. For further information on description of applications, see **HOPEX IT Architecture**.*

EXTERNAL ENVIRONMENT

This is the external environment in which the organization operates as well as its relationships with this environment. For example, this can include:

- The business, social, regulatory, cultural, competitive, financial and political environments of the organization
- The list of regulations that impact the organization and the associated requirements
- The strengths, weaknesses, opportunities and threats of the organization
- External stakeholders and their requirements
- Key performance indicators

Establishing the external context ensures that external org-units and their objectives and requirements are considered for the development of risk management policies.

To describe the external environment in which the organization operates, **HOPEX Risk Mapper** enables you to define:

- The list of regulations that impact the organization and the associated requirements, see "Regulation Frameworks", page 18,.
- The list of external stakeholders of the organization and their objectives and requirements, see "External org-units: objectives and requirements", page 23.

Regulation Frameworks

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

Accessing the regulation frameworks of the organization

To access the regulation frameworks with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks** navigation window, then expand the folder that corresponds to your repository.
The **Regulation Frameworks** and **Control Systems** folders appear.
2. Expand the **Regulation Frameworks** folder.
The list of regulation frameworks for the organization is displayed.

    ☺ *You can import into your repository libraries containing description of a regulation framework with its associated requirements, risk types, risk factors and control types.*

    ☛ *There can also be regulation frameworks internal to the organization serving as a guide to governance. In this documentation, the terms "Regulation" or "regulation framework" are used to refer to both internal and external regulations.*

Create a regulation framework

To create a regulation framework with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks**.
2. In the pop-up menu of the "Regulation Frameworks" folder, select **New > Regulation Framework**.
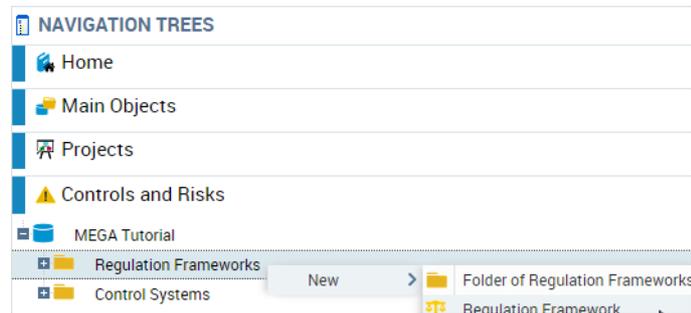
A dialog box asks you to enter the name of the new regulation framework.

3. Having entered the name, click **OK**.
    The new regulation framework appears in the navigator menu tree.

Regulation framework characteristics

To access the general characteristics of a regulation framework:

1. Open the properties dialog box of the regulation framework.
2. Click the **Characteristics** tab.
    The characteristics are as follows:

   -   The **Regulation Code** , which is internal,
   -   **Regulation Scope**, which can be international, local, a country or group of countries, etc.
   -   **Regulation Date**, open-ended text that specifies the year or application period of the regulation
   -   **Application Begin Date** of the regulation
   -   **Application End Date** of the regulation
   -   **Regulation Status**

        ☛ *the **Regulation Status** appears grayed and cannot be modified since it is managed by the workflow associated with the regulation framework. For more information, see **HOPEX Internal Control**.*

   -   The date of the **Last Update** of the regulation.

Regulation framework classifications

To access the classifications of a regulation framework:

1. Open the properties dialog box of the regulation framework that interests you and click **Classification**.

2. You can select a classification from among the following:
- Risk types, see "Risk types", page 21;

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

- Risk factors, see "Risk factors", page 22;

  📖 *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.*

- Control types, see "Control Types", page 22.

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

3. If you select **Risk Types**, for example, the list of risk types associated with the regulation framework appears.

```
⊟ ⚖  Basel II 2004
   ⊞ 📁   Requirements
   ⊞ 📁   Risk Factors
   ⊟ 📂   Risk Types
      ⊞ ⚠    B04 1 Internal fraud
      ⊞ ⚠    B04 2 External fraud
      ⊞ ⚠    B04 3 Employment Practices and Workplace Safety
      ⊞ ⚠    B04 4 Clients, Products & Business Practices
      ⊞ ⚠    B04 5 Damage to Physical Assets
      ⊞ ⚠    B04 6 Business disruption and system failures
      ⊞ ⚠    B04 7 Execution, Delivery & Process Management
```

Regulation framework requirements

To access the requirements of a regulation framework:

❯ Open the properties dialog box of the profile that interests you and click **Requirements**.

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

Control systems of a regulation framework

  📖 *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: the quality control system, the control system relating to IT and Privacy, the management control system, the internal audit system.*

  ☛ *For more details on control systems, see "Control Systems", page 25.*

Risk types

By grouping similar potential events, managers can improve their procedure for identifying opportunities and risks.

Enterprises can also classify potential events to ensure that the efforts deployed for identification are exhaustive. This classification can also contribute to subsequent development of an overview of risks.

     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.

Breakdown of risk types will be specific to activities and will depend on the particular business line or activity. Generic risk types can be broken down to a greater or lesser extent into specific risk type levels.

It is important to have a risk type definition framework that is identifiable, measurable and manageable, and to limit the number of levels to assure usable nomenclature.

Validation of nomenclature should ensure that a risk defined in two different entities or activities will have the same definition and the same sense, therefore ensuring system consistency.

In that the system installed should also meet regulatory requirements, it will also be necessary to define a second nomenclature to meet declaration aspects and to enable exchanges with control authorities.

```
For example, in the banking sector, risk types have been
defined in the context of Basel II recommendations. For more
details, see http://www.bis.org/bcbs/ HOPEX enables
handling of these risk types.
```

To create your own risk types with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks** navigation window, then expand the folder that corresponds to your repository.
    The **Regulation Frameworks** and **Control Systems** folders appear.
2. Expand the **Regulation Frameworks** folder.
    The list of **Risk Types** appears.
3. Click on the title bar of the **Risk Types** folder, select **New > Risk Type.**.
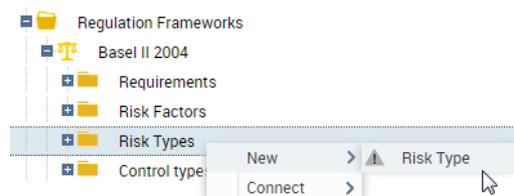
4. Enter the name of the risk type and click **OK**.
   The new risk type appears in the navigator menu tree.

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

   ☞ *To create your own risk types with the **Risk Manager (simplified)** profle in the **Risk Library** tab, select **Risks > Categories > Risk Types**.*

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.*

To access the list of risk factors with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks** navigation window, then expand the folder that corresponds to your repository.
   The **Regulation Frameworks** and **Control Systems** folders appear.
2. Expand the **Regulation Frameworks** folder.
   The risk factor tree appears.

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 create your own risk types with the **Risk Manager (simplified)** profle in the **Risk Library** tab, select **Risks > Categories > Risk Factors**.*

Control Types

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

   A control nomenclature frequently used is that defined by the COBIT.

   COBIT signifies "Control Objectives for Information and Related Technologies" .

   COBIT is a framework of best practices that now integrates numerous other frameworks and has the support of a large number of world experts. Of the 34 processes defined in COBIT there are 318 corresponding control objectives for which detailed control practices have been identified. The proposed verification guide describes elements necessary for correct understanding of each process, specifies controls to be carried out, provides elements for

assessment of conformity to best practices and assessment
of risk of non-achievement of objectives.

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

To access the list of control types with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks** navigation window, then expand the folder that corresponds to your repository. The **Regulation Frameworks** and **Control Systems** folders appear.

2. Expand the **Regulation Frameworks** folder. The control type tree appears.

☞ *To create your own risk types with the **Risk Manager (simplified)** profle in the **Risk Library** tab, select **Risks > Categories > Control Types**.*

External org-units: objectives and requirements

📖 *An external org-unit is an external entity that exchanges flows with the enterprise. Example: customer, supplier, government office.*

Defining the various parties concerned by risks faced by the enterprise is important in the majority of activities. This analysis is generally necessary from the first steps of a risk management project.

External org-units to be considered can be:

- Legislators
- Government agencies, ministries and local administrations
- Interest groups such as ecological lobbies
- Emergency services
- Financial institutions and other private sector fund suppliers
- Customers of the organization, including their managers, executives and personnel
- Suppliers and sub-contractors
- Persons who may be affected by enterprise activities due to their geographical location
- The media

To access all the org-units of the organization, see "Organization of internal org-units", page 14.

To specify that an org-unit is external to the organization:

1. Open the org-unit properties dialog box and select the **Characteristics** tab.

2. In the **Internal / External** field, select **External Org-Unit**. The **External Org-Units** appear with a green icon in the diagrams and in the navigation trees.

RISK MANAGEMENT CONTEXT

The risk management project must acknowledge the enterprise objectives that are relevant to the project. It must also consider the necessity of balancing costs, benefits and opportunities.

    📖 *A project is a part of a system whose study is entrusted to the same team.*

    ☛ *For more details on projects, see "Risk Management Projects", page 24.*

The responsibility of management in relation to risks taken by their enterprise not only imposes the installation of control systems to enable risk management, but also their demonstration at audit and attachment to the corresponding paragraphs of regulations.

Control systems imposed by regulations (Sarbanes-Oxley Act, etc.), by clients (ISO 9000 certification), or by sectorial control systems (Basel II in the banking sector, etc.) can be superimposed on the *control systems* implemented in an enterprise

    📖 *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: the quality control system, the control system relating to IT and Privacy, the management control system, the internal audit system.*

Last but not least, the description of the internal context in which the risk management process operates can be supplemented by the description of existing *control systems*.

During risk management projects, existing control systems will be reviewed and new *control systems* may be created.

    ☛ *For more details on control systems, see "Control Systems", page 25.*

Risk Management Projects

    📖 *A project is a part of a system whose study is entrusted to the same team.*

A risk management project must be approached by taking into account the company objectives that are relevant to the project. It must also
consider the necessity of balancing costs, benefits and opportunities.

Defining a risk management project involves:
- selecting the strategic **objectives** and requirements relevant to the project
- defining the **objectives** specific to the project
- determining the resources available for the project (capital, persons, systems, etc.)
- selecting from among existing **control systems** those that are concerned by this project
- defining the new **control systems** to be installed
- defining the project scope: org-units, sites, processes and systems concerned, for instance.

During risk management projects, existing control systems will be reviewed and new *control systems* may be created.

☛ *For more information on project management, see **HOPEX Common Features**.*

Control Systems

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

To access the list of control systems with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks** navigation window, then expand the folder that corresponds to your repository. The **Regulation Frameworks** and **Control Systems** folders appear.
2. Expand the **Control Systems** folder.
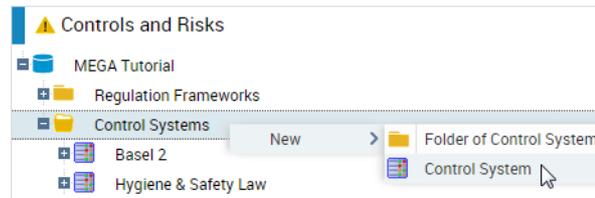   The list of control systems defined in the database appears.

With each control system can be associated *requirements*, *risk types*, etc.

Creating a control system

To create a control system with the ***Control and Risk Architect*** profile:
1. From the **Repository** paint, select **Controls and Risks**.

2. In the "Control Systems" folder pop-up menu, select **New > Control System**.

A dialog box asks you to enter the name of the new control system.
3. Having entered the name, click **OK**.
The new control system appears in the navigator menu tree.

Control system characteristics

To access the characteristics of a *control system*:
1. Open its properties dialog box from its pop-up menu.
2. In the properties dialog box that opens, select the **Characteristics** tab.
For a control system you can enter:
- The **Control System Code**
- The **Control System Audit Periodicity**.
- The **Regulation Frameworks** to which the control system makes reference.

Control system scope

In the **Scope** tab of the control system properties dialog box, you can indicate the *applications*, *business functions*, *processes*, *org-units*, *sites*, etc. concerned by the control system.
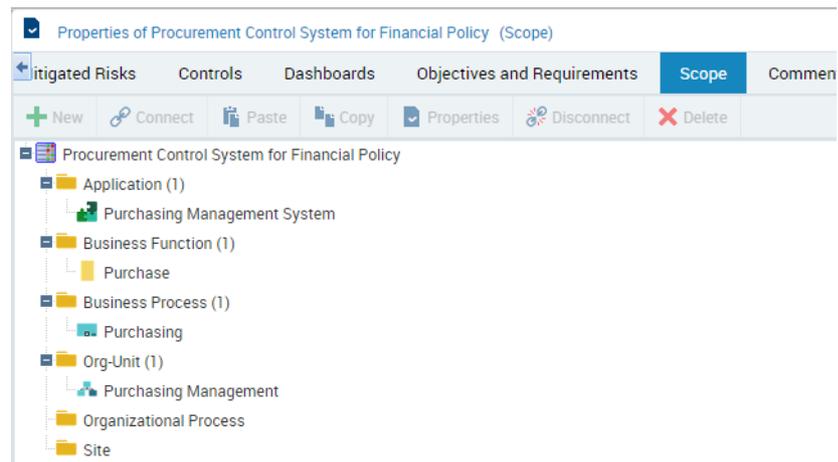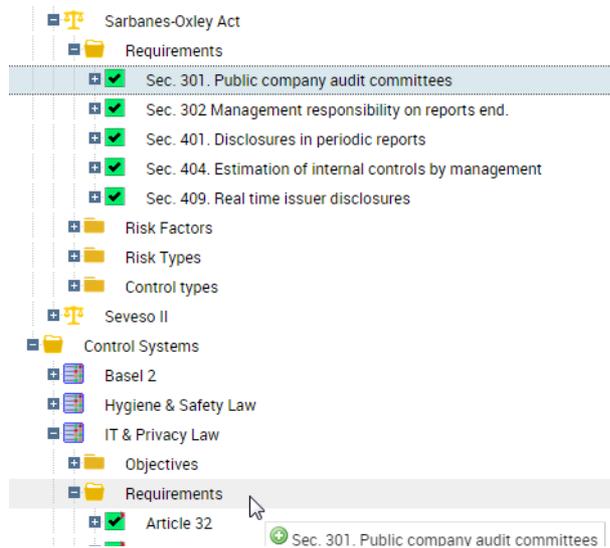
Control system requirements

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

With the ***Control and Risk Architect*** profile, you can select, from the *requirements* associated with *regulation frameworks* to which the control system refers, those relevant to this *control system*.

To do this:

❱ In the navigator, copy the requirements of interest and paste these in the "Requirements" folder of the control system.

You can also add requirements specific to the particular control system.

To create a requirement with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Controls and Risks**.
2. In the "Control Systems" folder pop-up menu, select **New > Requirement Pass**.
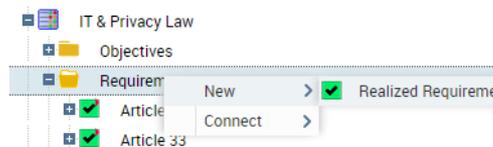
3. Enter its name and click **OK** to include this new requirement in the list of control system requirements.

Control system objectives

You can find *objectives* and *requirements* of the control system in the **Objectives and Requirements** tab of its properties dialog box.

📖 *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.*

Classifications

The different classifications (*risk factors*, *risk types*, *control types*) associated with a control system are accessible from the *control system* dialog box and from the navigator.
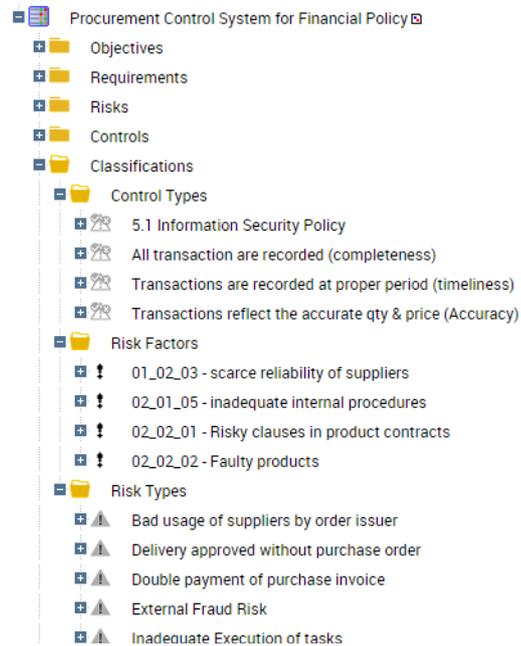
As for *requirements*, you can select from among the classifications associated with *regulation frameworks* those that are relevant to this control system.

ASSESSES RISKS

To control risks, you must be able to assess them. It is therefore necessary to identify and qualify the risks encountered in the execution of a business process. To do this, **HOPEX Risk Mapper** enables management of the risk concept.

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

Enterprise is confronted with numerous risk types: financial, legal, ecological, IT, technical, commercial, contractual, etc.

   ✓ The decision to manage or not each risk can be based on criteria that include operational, technical, financial, legal, social and humanitarian considerations. These criteria reflect the context defined by the project. They often depend on an organization's internal policies, goals and objectives and the interests of stakeholders.

Risk evaluation and treatment methods must be chosen in compliance with project objectives and requirements. Risk determination and evaluation can combine several complementary approaches. These can be based on:

   ✓ enterprise objective achievement
   ✓ application of predefined lists of risk types, risk factors or control types to their appearance context (process, activity, etc.).
   ✓ historical data (databases of incidents, claims, faults, etc.).

In **HOPEX Risk Mapper**, there are different types of object linked to risks:

    • Object types that could be at risk (for example: *business process*, *application*, *operation*, *, org-unit*, etc.).
    • Object types that enable processing of an incident or taking preventive measures (*control*, *process*).

The following points are covered here:

IDENTIFIES RISKS

When the control internal environment has been defined and enterprise objectives in terms of risk have been specified, the step of identification of events at risk starts.

Risk identification is generally carried out within the framework of a specified *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: the quality control system, the control system relating to IT and Privacy, the management control system, the internal audit system.*

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

Risk Identification Methods

The identification of risk events involves the inventory of the internal and external events that could compromise the achievement of objectives. A distinction must be made between those that represent risks, those that constitute opportunities and those that result from both simultaneously. Opportunities are integrated in the strategy of the organization or in the objective setting procedure.

Risk events can be identified using several approaches that involve operational management to differing degrees.

Method based on risk type or risk factor lists

It is possible to start by defining a list of generic risks faced whatever the activity. In particular, this includes natural disaster, IT system failure, human error, fraud, etc.

An initial list drawn up by a central team will avoid a complete analysis of risks with business function operational managers, to concentrate on risks that are specific to their activity. This list could be based on regulatory texts and lists provided by professional partners (professional associations, insurance companies, etc.).

This list can then be completed during interviews with operational managers of processes who can define the types of risks to which they are vulnerable to give a precise definition.In this case you identify the processes and the stakeholders or org-units of the organization concerned by these risk types or these risk factors.

A risk identification questionnaire is prepared, from which each stakeholder selects risk types and risk factors of particular concern.

A questionnaire can therefore be produced and sent to the various stakeholders to enable them to identify risk events that concern them.

☞ *See **HOPEX Assessment** for more information on questionnaires.*

Replies to these questionnaires are then analyzed by experts in each of the subjects concerned, in consultation with the stakeholders concerned if necessary, to finalize risk identification.

It is then possible to remove from this generic list, which has been supplemented by risks specific to the activity, those risk events that do not apply to the particular field (example: a purely manual activity that does not require the services of an IT system.

Method based on enterprise objectives and business process diagrams

It is possible to determine the risks of not achieving organization objectives or not satisfying regulatory or organization internal requirements using the description of organization business processes.

To do this, we select the processes that contribute to achieving these objectives or satisfying these requirements. Next, determine the risks by analyzing the flows exchanged between the org-units participating in these processes as well as the operations executed by these org-units. From among these flows and operations, determine which ones could, in the event of malfunction, prevent the achievement of objectives or the satisfaction of requirements of the organization.

This approach can be supplemented by using other risk identification criteria such as risk type or risk factor lists if these are available.

If enterprise business process diagrams already exist, they can help to identify risks.

Risk events can be associated with each of the modeled processes.

Risks associated with a process are visible in the **Risks** tab of the properties dialog box of the process.

Local name	Impact	Likelihood △
Favoritism in selection of suppliers	Medium	Possible
Goods receipt inconsistant with purchase order	Very High	Probable
Creation of an imaginary supplier	High	Rare

☛ *Risks can be linked to other concepts such as org-unit, application, etc.*

Method of identification from incidents repository

All types of stored history can be used, such as repositories of incidents, faults, claims, etc.

Identification consists of analyzing repositories to determine risk events. You should then specify for each risk its appearance context (business process, organization org-unit, IT application, enterprise site, etc.).
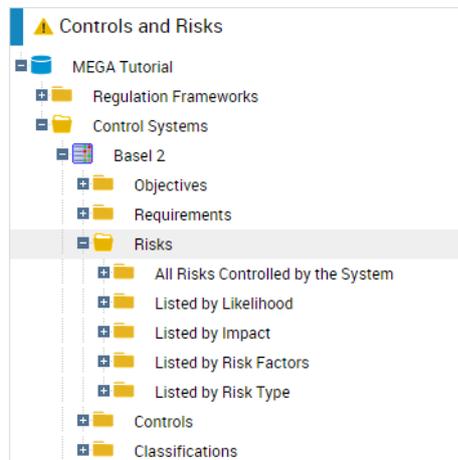
☛ *See the **HOPEX LDC** user guide for more information on incidents (events) repository management.*

Accessing risks

With the **Control and Risk Architect** profile, you can access risks via control systems.

To access risks with the **Control and Risk Architect** profile:
1. Click **Controls and Risks > Control Systems.**
2. Select a control system and click the **Risks** folder.

☛ *The risks mitigated (limited) by a control system can be viewed in the **Mitigated Risks** section of the control system properties window. For more details, see "Control Systems", page 25.*

To access risks with the **Risk Manager (simplified)** profile:

❭ Select **Risk Library > Risks > All Risks**.

☛ *To access the most important risks: Click **Environment > Risks > Key Risks**.*

Creating risks

The procedure for creating a risk varies according to the profile you are using.

To create a risk associated with an organizational process with the ***Control and Risk Architect*** profile:

1. From the **Repository** paint, select **Main Objects**, then unfold the**Business Process** folder.
2. Open the properties window of the product that interests you.
3. Select the **Risks** tab.
4. Click the **New** button.
   The risk creation dialog box appears.

To create a risk with the ***Risk Manager (simplified)*** profile:

1. Select **Risk Library > Risks > All Risks** and select **Risks > All Risks**.
2. Click the **New** button.
   The risk creation dialog box appears.

Risk characteristics

In the **Characteristics** section of the risk properties window, you can specify the following characteristics:

- the risk identification **Code**
- the risk **Name**
- the fact that the risk is high level by selecting the **Key Risk** check box
- the risk **Owner**.

  ☛ *By default the **owner** is the risk creator.*

- the risk **Identification Mode**
  The risk could have been identified from:
  - an "Incident database"
  - a "Workshop"
  - a "Survey"
  - a "Mission audit"
- the risk **Description**

  ☛ *the **Risk Status** appears grayed and cannot be modified since it is managed by the workflow associated with the risk. For more information, see **HOPEX Enterprise Risk Management**.*

Risk scope

Risk scope enables definition of risk location. It relates to several component types:

- **Business Processes** and **Organizational Processes** exposed to the risk. For more details, see "Organization Processes", page 16.

  📖 *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.*

- **Entities** concerned by the risk. For more details, see "Organization of internal org-units", page 14.

  📖 *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.*

- **Objectives and Requirements** expected related to risk management. For more details, see "Organization objectives and requirements", page 15.

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

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

- **Applications**: for more details, see "Applications", page 17.

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

- **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.*

- **Operations**

  📖 *An operation is an elementary step in an organizational process executed by an org-unit.*

  🖋 *In the **HOPEX Control and Risk** product, a **Situation** tag is available to define the scope of a risk. Use the compatibility option to reuse information that was defined in this tab to integrate it in the **Scope** of the control. To activate the accounting option, see "Managing Options Relating to Risks", page 5.*

RACI on a risk

A risk properties page includes an **RACI** section to define the different persons responsible for risk management.

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

Responsibility levels

The proposed responsibility levels are as follows:

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

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

- on a risk,
- on a control.

Specifying Responsibilities

With **HOPEX Risk Mapper**, persons are represented by **system persons**.

📖 *A system person represents a person in the enterprise. This person can be assigned a login and a role (or a profile depending on the connection mode). The login provides access to the HOPEX Application. The role (or the profile) defines the access to product functions and repositories. A system person, if assigned a login, has a specific desktop in each database, and can connect to this desktop from any workstation in a given environment.*

To specify the persons responsible for a specific object:

1. In the object properties page, expand the **RACI** section.
2. Connect the system persons in each of the following tabs:
   - **Responsible**
   - **Accountable**
   - **Consulted**
   - **Informed**.

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

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

RISK ANALYSIS

The aim of risk analysis is to obtain a good understanding of risks. It offers elements that help to decide on whether treatment of a risk is necessary, and to select the most appropriate and cost-competitive treatment strategies. Risk analysis must take risk sources into account as well as positive or negative risk consequences.

The analysis phase associates a risk with:

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

Contextualization of a risk enables risk classification by:

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

The same risk can relate to several component types specified in the risk scope:

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

☛ *These components are specified in the risk characteristics, in the* ***Scope*** *section. For more details, see "Risk scope", page 33.*

Risk analysis

To analyze a risk:

1. Select a risk and open its properties.
2. In the **Characteristics** tab, expand the **Analysis** section.
   A risk is characterized by:
   - **Control System(s)**: for handling risk management, see "Control Systems", page 25.
   - **Risk Types**: for more details, see "Risk types", page 21.

     📖 *A risk type defines a risk typology standardized within the context of an organization.*
   - **Risk Factors**: for more details, see "Risk factors", page 22.

     📖 *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.

- **Risk Consequences**: for more details, see "Risk consequences", page 37.

  📖 *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.*

  ☞ *See the **HOPEX LDC** user guide for more information on incidents (events) repository management.*

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 consequences associated with a risk:

1. Open the properties page of a risk and select the **Characteristics** tab.
2. Open the **Analysis** section.
3. Select the **Risk Consequence** tab and the **New** tab.
   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.*

Cause-and-Effect Diagram

Analysis of the most important risks can be completed with the help of a cause-and-effect diagram to describe the sequence of its causes and/or its effects. This study could reveal new risks or risk factors.

A Cause-and-Effect diagram, also called a "Ishikawa Diagram" or a "Fishbone Diagram" enables description of a sequence of causes and effects for problem or issue analysis.
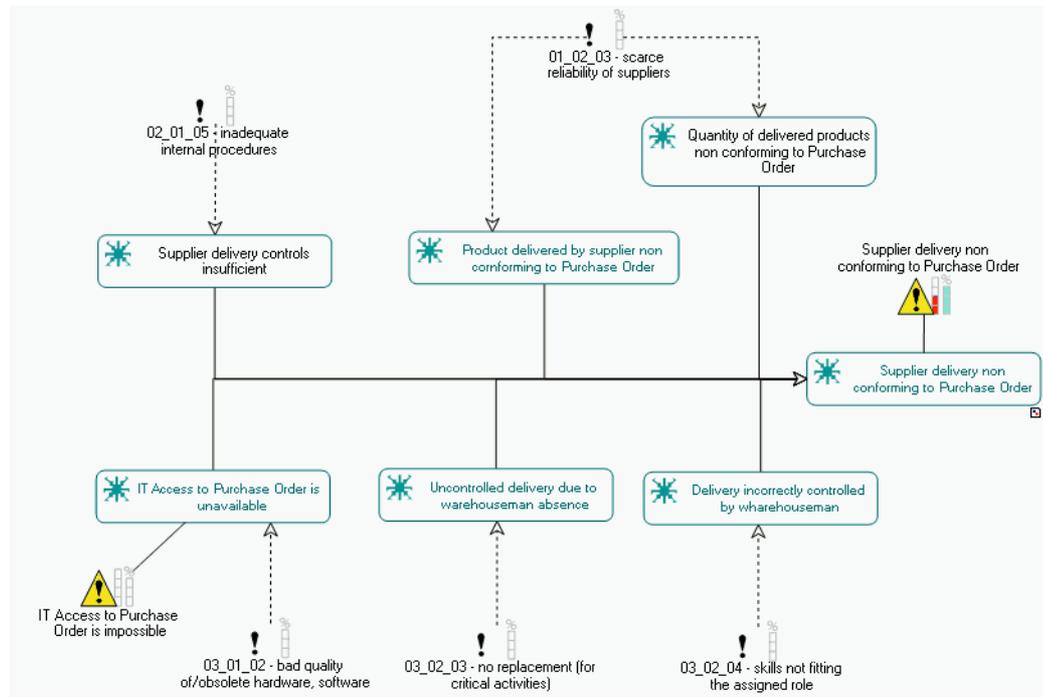
Cause-and-effect diagram

In the above example, we analyze possible causes of the "Supplier delivery non-conform to purchase order" risk.

We list possible causes of the problem, and for each cause we specify the corresponding risk factors. At this point it is possible to identify new risks.

☛ *For more information on the cause-and-effect diagram, see "Cause-and-Effect Diagram" in the chapter "Objectives and Requirements" in* ***HOPEX Common Features****.*

☛ *In **HOPEX Common Features**, issues and problems are equivalent concepts.*

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

HOPEX Risk Mapper offers the possibility of a direct assessment, which allows an expert to specify global assessment of a risk on a given date,

Results of risk assessment can be displayed in dedicated reports whick make it easier to analyse the assessed risks. For more details, see "HeatMaps", page 63.

Assessing risks directly

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

You can carry out:
- direct assessment from a risk
- multiple assessment from a table

Creating direct assessments

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

This is an "expert view" assessment.

To create an assessment:
1. Select a risk and open its properties.
2. Select the **Assessment** tab.
3. Click the **Evaluate** button.
4. Select the entities for which the risk is to be assessed, then click **Next**.
   - ☛ *The contexts are available only if there is more than one.*
5. Specify characteristics values:
   - **Impact**: the impact of the risk when it occurs.
   - **Likelihood**: the probability that the risk will occur.
   - **Control levels**
6. Specify the assessment date.
7. Click **OK**.
   An assessment is created.

Representation in a Diagram

To display risks in a diagram with their likelihood and impact:

❱ Select **View > Views and Details** and select the "Risks" view.

In the objects toolbar, the risk is represented by the "Danger" triangle ⚠

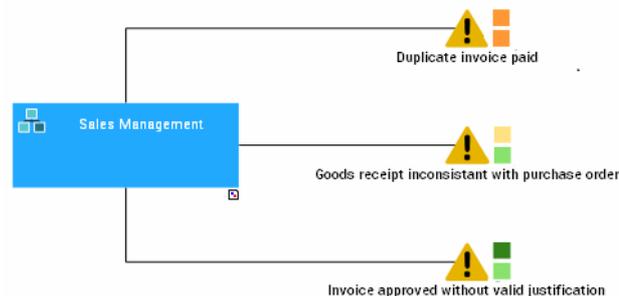The colors to the side of the "Danger" panel vary according to the values resulting from the risk assessments.

Impact: medium, Likelihood: possible

Impact: very low, Likelihood: possible

Risks can be displayed in the diagram with colors that indicate their impact and likelihood.

Risk Summary

HeatMap by Entity/Risk Type/Process

When the likelihood and the impact of a risk have been specified, you can obtain a summary view of risks to highlight the risks to be treated as a matter of priority.

To do this, see "HeatMaps", page 63.
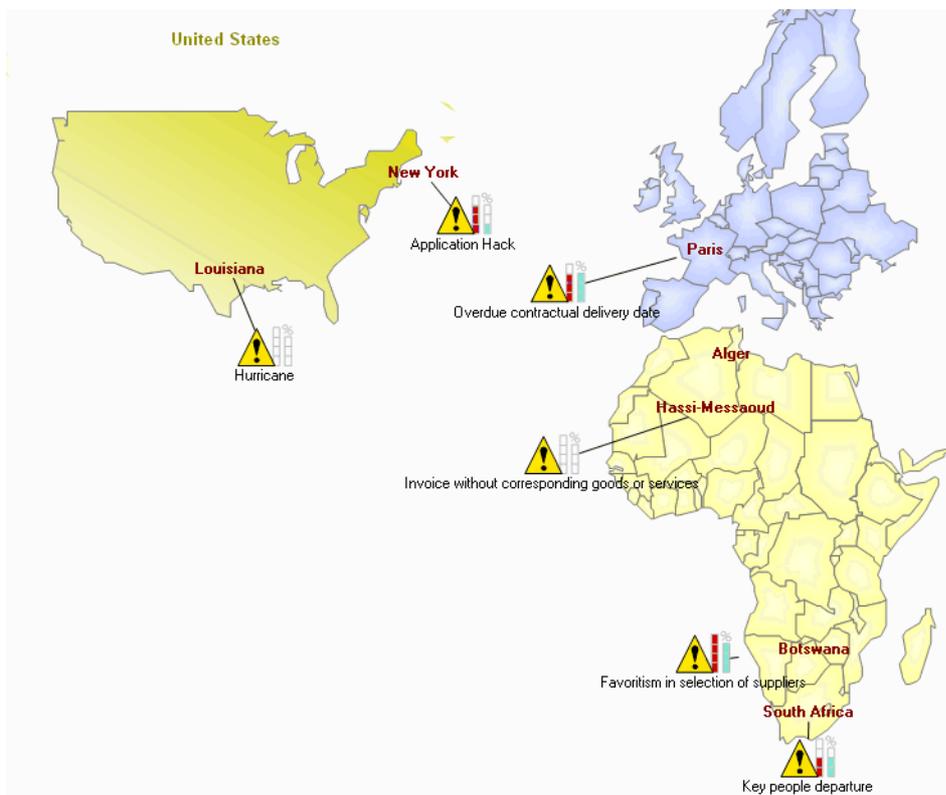
Risk geographical map

It is also possible to describe the geographical distribution of control system risks.

To do this:

> ❱ Create a geographical map of control system risks or open an existing map.

The geographical map of risks is displayed.

It allows you to connect risks to the sites where they may occur.

Risk Mapper on HOPEX

RISK TREATMENT AND CONTROLS

The assessment of risks produced a list of risks that could require treatment, with their estimation and order of priority.

Treating risks involves the identification of the various options possible, assessment of these options and the preparation and implementation of treatment plans.

Before determining the appropriate treatment actions, it can be useful to review the risk analysis and extend it to obtain the information required for identifying the different treatment options. The design of risk treatment measures should be based on a perfect understanding of the risks concerned; this understanding is obtained from an appropriate level of risk analysis. It is particularly important to identify risk causes so that the risks themselves will be treated and not just their symptoms.

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

RISK TREATMENT

When risks have been analyzed and assessed, management determines how each of these risks should be treated.

To specify risk remediation choices:

> ❱ Open the properties page of a risk and select the **Remediation** tab.

Risk Control Level Selection

Target risk

For a given risk, you can define the level of risk acceptable for the organization.

    📖 *The target risk presents the residual risk value expected by the risk manager after treatment of the risk.*

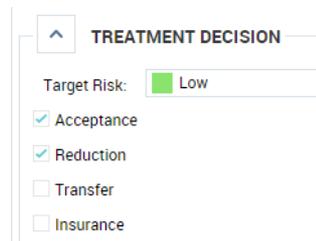If this risk level is higher than or equal to the previously assessed risk, the organization can accept the risk as it stands.

Control Level Selection of a Risk

For each risk identified, a level of risk acceptable to the organization must be defined.

If the risk cannot be accepted as it stands, various solutions for facing the risk can be proposed.


- **Acceptance**
  The risk is accepted and no action is taken to try to reduce the risk.
- **Reduction**
  Risk likelihood can be reduced by installing additional controls, or the severity of its consequences can be reduced if the risk occurs.
- **Transfer** (sub-contractor)
  The risk can also be shared with other partners, in particular when they have greater skills in controlling the risk. For example, you can sub-contract a dangerous activity to a partner specialized in the particular field. In such cases, it should be noted that it is often necessary to carry out a new risk study, since the introduction of a new partner can bring additional risks.
- **Insurance**
  To supplement all the above approaches, it is often necessary to resort to insurance, in particular for risks of low likelihood but with high severity. In such cases, the insurer will generally request that risk prevention and reduction measures also be implemented.

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

Depending on the solution adopted, the effect of the different solutions in terms of likelihood and impact should be considered, as well as costs and benefits.

The choice should be the solution that reduces residual risk to within the tolerance limit required by management.

A comment allows you to specify the risk treatment method.
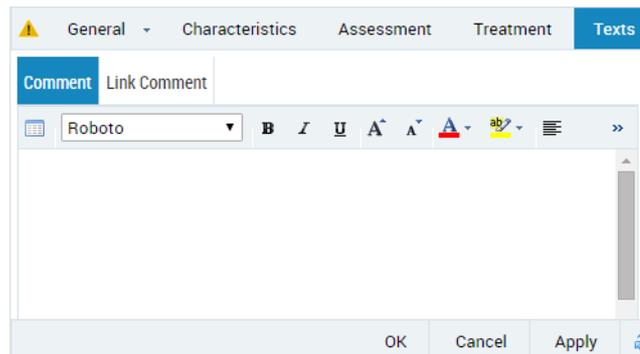
Specification of Actions to be Implemented

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

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

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

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

To indicate the **Controls** and **Action Plans** enabling risk prevention:

❱ In the **Remediation** tab of the risk properties page, expand the **Controls and Action Plans** section.

- The **Action Plans** tab contains the list of action plans installed: for example for creation or improvement of a control, management of a crisis linked to occurrence of an incident, or revision of a process with a view to its improvement. See "Implementing Action Plans", page 47.

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

- The **Controls** tab lists controls planned for risk reduction. See "Risk prevention controls", page 47.

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

Risk prevention controls

Installation of prevention controls to reduce risk likelihood and impact can be a solution for risk reduction.

To indicate the controls that enable risk prevention:

❱ Click on the risk and select **Connect > Preventive Control**.

☛ *For more details on implementation of controls, see "Controls", page 48.*

Implementing Action Plans

The use of action plans is available with the **HOPEX Enterprise Risk Management** product.

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

☛ *For more information on use of action plans, see **HOPEX Enterprise Risk Management**.*

CONTROLS

Control activities comprise policies and procedures that enable assurance that risk treatment required by management has been effectively implemented. Control activities are present throughout the organization, at every level and in every function. They also include a range of varied activities such as validation, authorization, verification, data mapping, operational performance review, assets security and task assignment.

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

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

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

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

- the object types enabling indication of the framework within which the control is installed (*control system*, *control type*, associated *requirement* or *risk*).
- the object types enabling indication of control implementation means (*process*, *application*, *operation*, *service*, *constraint* our *resource*, etc.).
- the object types enabling indication of control implementation responsibilities (*org-unit*, *person*).

> ☞ *Operation and service object types are available with **HOPEX Business Process Analysis**.*

Control Identification

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

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

- From risks
  Certain controls are installed to meet a particular risk.

- From control type lists
  Control type lists are associated with certain regulations (eg.: COBIT).

- From diagrams of existing business processes
  Similarly to risk identification, it is possible to examine the operation of each step in the business process from its diagram, if this exists, to discover the controls installed.

- From specialist expertise
  A specialist in a particular field is often able to describe controls which are or should be implemented.

- From incident databases
  By consulting past events, controls that could have prevented them or reduced their consequences can be proposed.

Access to Controls

To access controls with the ***Control and Risk Architect*** profile:

1. Click **Controls and Risks > Control Systems.**
2. Select a control system and click the **Controls** folder.
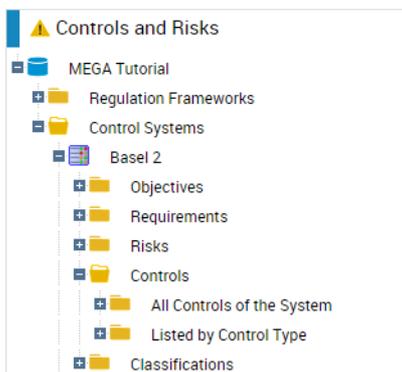
☞ *To access your own controls with the **Risk Manager (simplified)** profile: in the **Risk Library** tab, select **Risks > Categories > All Types**.*

As with risks, associated controls can be numerous. To improve control management, **HOPEX Risk Mapper** proposes several control classification criteria.

☞ *The risks mitigated (limited) by a control system can be viewed in the **Controls** tab of the control system properties window. For more details, see "Control Systems", page 25.*

Control characteristics

In the **Characteristics** tab of control properties, you can specify:

- its **Code** enabling unique identification of the control
- **Name**
- **Owner**

  ☛ *By default the **owner** is the control creator.*

- control importance if required, by selecting the **Key Control** check box.
- the **Level**, see "Control level", page 50
- the **Control Nature**, see "Control nature", page 50
- the **Execution Mode**, see "Control Execution Mode", page 50
- the **Frequency** (see "Control Execution Mode", page 50).

Control level

Control level enables the distinction to be made between "operational" and "organizational" controls.

- level 1 - operational
  Operational level controls are those executed during the normal operation of enterprise business processes.
- level 2 - organizational
  Organizational level controls are then carried out periodically by management to check that operational processes have been correctly executed and that their results comply with requirements.

Control nature

This characteristic concerns the motives of the control:

- Correction
- Detection
- Prevention

Control Execution Mode

This characteristic enables the specification of the way in which the control is executed:

- Observation
- Control by survey
  The control is executed on random samples.
- Systematic control
  The control is executed systematically and exhaustively on all objects treated.

Control Execution Mode

Control execution periodicity can be systematic, daily, weekly, monthly, etc.

RACI on a control

A control properties page includes an **RACI** section to define the different persons responsible for control management. For more details, see "RACI on a risk", page 35.

Control scope

You can define the control more precisely by indicating the risks, processes, entities and requirements that are attached to it.

To define control scope:
1. Open the properties page of a control.
2. Expand the **Scope** section.
   The following tabs are available:
   - **Risks** covered by controls. For more details, see "Assesses risks", page 29.

     *In the **HOPEX Control and Risk** product, a **Risks Controlled** tab indicates which risks or risk factors are prevented by the control. Use the compatibility option to reuse information that was defined in this tab to integrate it in the **Scope** of the control. To activate the accounting option, see "Managing Options Relating to Risks", page 5.*
   - **Business Processes** and **Organizational Processes** exposed to risks covered by the control. For more details, see "Organization Processes", page 16.
   - **Entities** concerned by controls. For more details, see "Organization of internal org-units", page 14.

Analyzing Controls

You can define the control more precisely by indicating the control systems that are attached to it.

The *control types* enable specification of regulation frameworks that apply to a given control.

☛ *For more details, see "Control Types", page 22.*

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

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

☛ *For more details, see "Control Systems", page 25.*

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

Control Objectives and Requirements

The **Objectives and Requirements** tab enables indication of the organization *objective* or regulatory or legal *requirement* met by the control.

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

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

Control Implementation

Installation of a control frequently consists of checking that a management rule (*constraint*) is effectively applied, either manually or by an IT program.

  A constraint is a declaration that establishes a restriction or business rule that must be applied on execution of processing.

You can specify the management rules associated with a control in the **Management Rules** tab of its properties page.

The control can be implemented by:

- a *process*: this can be the business process on which the control is implemented or it can be a risk preventive business process (example: "Account manager training" to prevent the "Overselling" risk)

  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 *operation*: this is the operation on which the control is executed.

  An operation is a step in a process, executed by an org-unit within the context of an activity. An operation can be industrial (manufacturing a component), logistical (receiving a delivery), or can involve information processing (entering an order). An operation can be subdivided into elementary tasks.

It is possible to specify processing that will implement the control or the management rules associated with the control. You can specify control implementation means in the **Characteristic** tab, **Scope** section.

3

Risk Control Policies Operational Monitoring

Policies and procedures are established and implemented to help ensure that risk responses are effectively carried out.

Monitoring is accomplished through ongoing management activities, independent assessments, or both.

CONTROL SYSTEM ONGOING IMPROVEMENT

Malfunctions identified via permanent operation monitoring or during periodic reviews are referenced and analyzed. Corrective actions are then planned and implemented.

- Malfunction identification
  The malfunctions to be examined are identified using a number of available sources: the initial remediation plan, feedback on risk remediation and incidents in installed control systems, and periodic reviews by operational management.

- Malfunction analysis
  Malfunctions are studied to deduce risks faced by the organization. These are then analyzed as previously discussed by determining risk factors with the possible help of a cause-and-effect diagram.

- Risk treatment implementation
  When the risk treatment actions to be undertaken, the control data storage requirement, and the risk measurement indicators to be implemented have been determined, an action plan including the necessary resources, budgets, deadlines and implementation managers is defined.

- Risk treatment action plan monitoring
  The frequency and terms of risk treatment plan monitoring are established.

The **HOPEX** repository enables the definition of controls carried out during enterprise business process execution, and the specification of which organizational, IT or human resources will implement them (see "Risk Treatment and Controls", page 43).

HOPEXalso allows you to describe procedures for feedback of information from the controls carried out during enterprise business process execution (see **HOPEX Business Process Analysis** of the MEGA modeling suite).

> *In the HOPEX Control and Risk product, a Redundancy tab is used to specify that certain controls are redundant. Use the accounting option tab if necessary to reuse information that was defined in this tab to integrate it in the Scope of the control. To activate the accounting option, see "Managing Options Relating to Risks", page 5.*

CONTROL EFFECTIVENESS ASSESSMENT

In addition to the continuous monitoring of risks during normal operation of organization business processes, periodic reviews of risk management are carried out by operational managers to verify that new risks have not appeared and that the risk treatment strategies applied are still suitable and effective. To determine this, control self-assessment questionnaires can be used.

In addition to the operational management reviews, audits that are internal or external to the activity offer an outside view of organization operation, and can reveal new malfunctions.

Audit findings will usually indicate systemic weaknesses of the risk management system. Actions taken in response to audits should be focused on remedying the system and not just the symptoms.

☞ *For more information, see* **HOPEX Internal Control***.*

INCIDENT AND LOSS MONITORING

After implementing a risk management policy, continuous monitoring of risks incurred using regular measurement of a number of parameters (eg: pollution levels, available budget, etc.) must be established to verify its efficient operation.

This can be done in particular through incident database management. Each incident is listed here and the resulting losses are evaluated. In certain cases, it is enough to ensure that the incident monitoring activity has been correctly executed and that it has not produced results exceeding anticipated tolerance thresholds.

If new risks are identified at this point, they should be added to the list of risks managed by the organization. Operational managers or the risk management manager within the organization must take these into account at the next risk review.

☛   *For more information, see* **HOPEX LDC**.

Reports HOPEX Risk Mapper

HOPEX Risk Mapper offers risk analysis and follow-up functions.

> ☞ *For more details on operation of reports, see the HOPEX Common Features guide, "Generating Reports".*

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

The following points are covered here:

IDENTIFICATION REPORTS

Matrix of Risks Incurred by Org-Units

This report inventories risks incurred by a set of org-units.

> ☛ *For more details on the specification of risks incurred, see "Organizing Risks", page 16.*

Access path

To access this report with the *Control & Risk Architect* profile:

1. Click on the org-unit (or the risk) in question, and with its pop-up menu and select **Report Discovery**.
    The list of **Reports Available** appears in the edit area.
2. Open the **Risk Analysis** folder.
    The **Matrix of Risks Incurred by Org-Units** in the list of reports.
3. Click **Customize and Launch New Report** if you wish to add org-units or risks.

> ☛ *When a report template includes several required parameters, you must complete the report before launching it.*

> ☛ *To create this report with the **Risk Manager (simplified)** profile: in the **Reports** tab, select **Identification > Matrix of Risks Incurred by Org-Units**.*

Report parameters

Parameter	Parameter type	Constraints
Org-units exposed to risks	Org-Units	At least one object mandatory.
Scope of ana-lyzed risks	Risk	Not mandatory. If no value is given, all risks are analyzed.

Report example

The first part of the report presents the number of org-units connected to each risk.

```
In the example below:
- a risk is connected to 7 org-units
- a risk is connected to 2 org-units
- three risks are connected to 1 single org-unit.
```


Graphiques
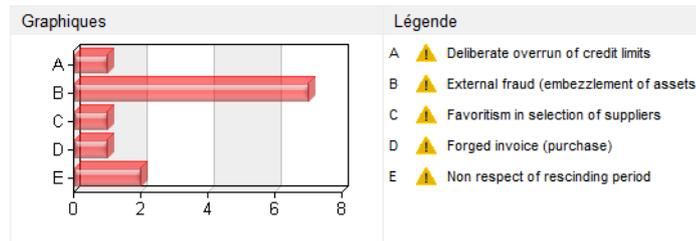
	Légende
A ⚠	Deliberate overrun of credit limits
B ⚠	External fraud (embezzlement of assets)
C ⚠	Favoritism in selection of suppliers
D ⚠	Forged invoice (purchase)
E ⚠	Non respect of rescinding period

Nombre d'acteurs analysés:80

Nombre d'acteurs exposés aux risques:11

Ratio:13.8

The second part of the report presents the matrix of links between the org-units and the risks that are part of the scope and that are connected to each other.

✔ Le risque peut impliquer directement l'acteur
✔ Le risque peut impliquer un sous-acteur.

	Deliberate overrun of credit limits ⚠	External fraud (embezzlement of assets) ⚠	Favoritism in selection of suppliers ⚠	Forged invoice (purchase) ⚠	Non respect of rescinding period ⚠
Account Manager	✔		✔		
Administration & Finances Management					✔
Buyer		✔			
Purchasing Assistant		✔			
Purchasing Manager		✔			
Agency		✔			
Boat Renting Agency		✔			
Customer		✔			

Matrix of Risks Concerning Sites

This report inventories risks incurred by a set of sites.

This is identical to the "Matrix of Risks Incurred by Org-Units", page 60 report; only the parameters vary.

Access path

To access this report with the **Control & Risk Architect** profile:

1. Click on the org-unit (or the risk) in question, and with its pop-up menu and select **Report Discovery**.
    The list of **Reports Available** appears in the edit area.
2. Open the **Risk Analysis** folder.
    The **Matrix of Site Risks** report in the list of reports.
3. Click **Customize and Launch New Report** if you wish to add org-units or risks.

    ☛ *When a report template includes several required parameters, you must complete the report before launching it.*

    ☛ *This report is not available to **Risk Manager (simplified)** users.*

Report parameters

Parameter	Parameter type	Constraints
Sites exposed to risks	sites	At least one object mandatory.
Scope of ana-lyzed risks	Risks	Not mandatory. If no value is given, all risks are analyzed.

HEATMAPS

HeatMap by Entity/Risk Type/Process

This report displays distribution of risks according to different criteria:

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

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

Access path

To access this report with the *Control & Risk Architect* profile:

1. From the **Repository** section, select **Documentation**, then unfold the **Reports** folder.
2. Right-click **HeatMap by Entity/Risk Type/Process** and select **New > Report**.
   The list of **Reports Available** appears in the edit area.
3. Open the **Risk Analysis** folder.
   The **HeatMap by Entity/Risk Type/Process** folder appears in the list of reports.
4. Click the **Complete** button.

> ☛ *When a report template includes several required parameters, you must complete the report before launching it.*

> ☛ *To create this report with the **Risk Manager (simplified)** profile: in the **Reports** tab, select **HeatMaps > HeatMap by Entity/Risk Type/Process**.*

Report parameters

This consists of defining report input data.

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

Report example

In the example below, no risk has been assessed.

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