HOPEX IT Risk Management

User Guide

HOPEX V2

INTRODUCTION

Each enterprise must implement governance and management processes for IT technologies.

HOPEX IT Risk Management is used to define and automate an appropriate governance system. This solution can be used to analyze risks using the current IT architecture and to define the level of control required to meet the objectives of the enterprise. **HOPEX**endeavors, in particular, to build a suitable control environment supporting enterprise business processes.

This solution is designed for IT departments and most particularly for risk, compliance and IT security departments.

- ✓ "Overview", page 8
- ✓ "Connecting to HOPEX IT Risk Management", page 10
- ✓ "Interface Presentation", page 14
- ✓ "About This Guide", page 15

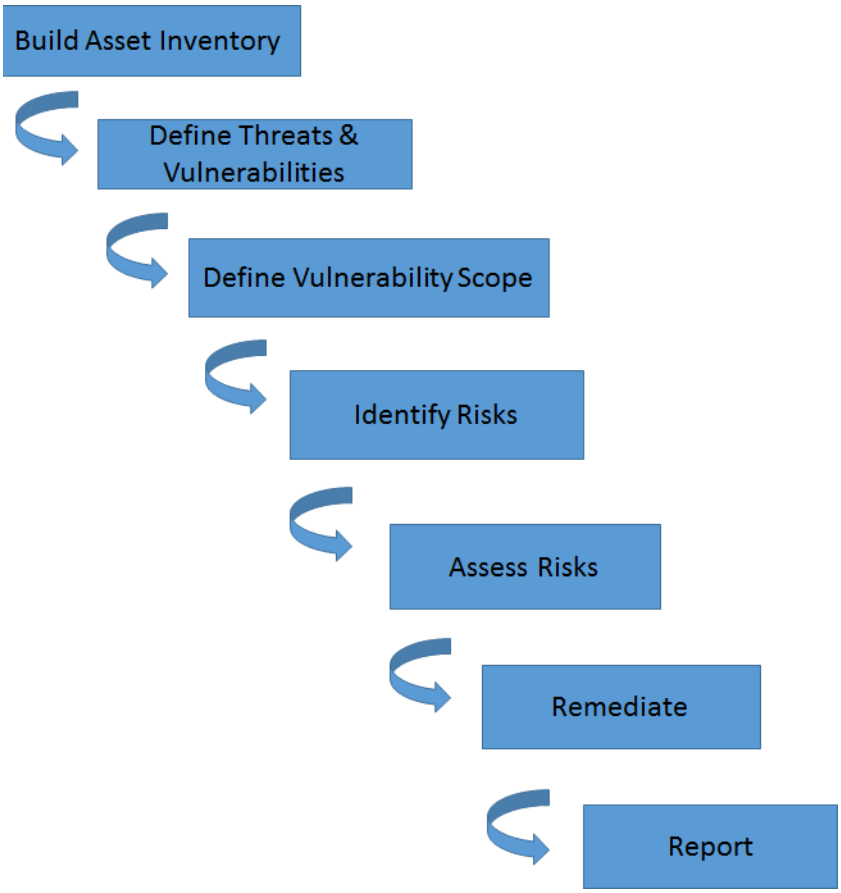
The following points are covered in **HOPEX IT Risk Management**:

- ✓ "Defining the Environment for Solutions", page 463
- ✓ "Managing inventories", page 17
- ✓ "Using HOPEX IT Risk Management", page 35
- ✓ "Assessments by Questionnaires", page 49

OVERVIEW

HOPEX IT Risk Managementis used to manage risks, compliance and IT vendors. You can capitalize on **HOPEX Architecture** or **HOPEX IT Portfolio Management** legacy inventories or enter them directly in the solution.

Business



Managing IT Risks

HOPEX IT Risk Management is used to:

- identify threats and vulnerabilities based on appropriate frameworks or information sources (for example: ISO 27005, CVE).
- produce reports concerning vulnerabilities and identify the risks that threaten IT assets.
- assess the risk level of IT assets, with an expert view or via questionnaires sent to application owners.
- identify the risk scenarios and the cause-and-effect links between risks.

Managing IT Compliance

IT departments must comply with a number of regulatory requirements and consequently deploy different types of controls on the IT assets.

HOPEX IT Risk Management is used to:

- identify the appropriate IT regulation frameworks (ISO 27002, NIST), the resulting requirements as well as the control types to implement.
- assess the control level (control design and efficiency) with an expert view or via questionnaires sent to application owners.
- produce reports illustrating the regulatory compliance level achieved.

Managing IT vendors

HOPEX IT Risk Management is used to:

- enter vendor commercial data
- launch assessment campaigns with a view to assessing the relationship with these vendors
- assess the global risk level represented by the vendor

CONNECTING TO HOPEX IT RISK MANAGEMENT

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

Running the Application

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

HOPEX IT Risk Management Solution Profiles

In **HOPEX IT Risk Management** , there are, by default, business profiles with which specific activities 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.*

IT RM functional administrator

The IT RM (IT Risk Management) functional administrator essentially manages environment objects (organization, process, business capacity, business line and IT asset inventory).

☛ *The application inventory can also have been previously built using **HOPEX Architecture** or **HOPEX IT Portfolio Management** by application portfolio and application managers.*

The functional administrator has access to the following desktops:

- **Administration**

  ☛ *For more details on this desktop, see **HOPEX Administration - Supervisor,** chapter "Accessing MEGA Administration".*

- **Environment**

  ☛ *For more details, see "Defining the Environment for Solutions", page 463.*

- **IT RM**

The main tasks of the manager are to:

- establish the application inventory
- establish the vendor inventories
- assign each application to one or more IT RM Manager
- assign, if required, applications to processes and/or business lines

IT GRC Manager

IT RM (IT Risk Management) managers are the main users of the **HOPEX IT Risk Management** solution.

They can belong to one or more departments (safety, compliance, risk management).

They have all rights over threats, vulnerabilities, risks, controls, assessment objects, regulations, requirements and reports.

The main tasks of the manager are to:

- establish the inventory for threats and vulnerabilities
- identify the vulnerabilities for each asset
- position risks on IT Assets
- assess risks
- define action plans for improvement

- identify regulatory requirements
- identify controls
- assess controls
- assess regulatory compliance

- enter the annual cost of products or services per vendor
- assess a vendor

Application owner

The application owner answers the questionnaire received in response to an assessment campaign.

The application owner can also consult the action plans assigned to him/her.

Summary of Rights by Profile

Rights concerning IT risks

For more details, see "Managing IT Risks", page 36.

	IT RM functional administrator	IT GRC Manager
Establishes the application inventory See "Inventory of IT Assets", page 18.	X	
Establishes the inventory for threats and vulnerabilities See "Inventory for Threats and Vulnerabilities", page 23.	X	X
Identifies the vulnerabilities for each asset See "Positioning Vulnerabilities on IT Assets", page 36.	X	X
Identifies and assess risks linked to IT assets See "Identifying and Positioning Risks", page 37, "Direct Risk Assessment", page 41.	X	X
Identifying Risk Scenarios See "Identifying Risk Scenarios", page 37.	X	X
Defining Action Plans for Improvement Purposes See "Treating risks", page 71.	X	X

Rights concerning IT compliance

For more details, see "Managing IT Compliance", page 44.

	IT RM functional administrator	IT GRC Manager
Identifies controls See "Identifying Controls on Applications", page 45.	X	X
Assesses the efficiency of controls See "Direct Control Assessment", page 45.	X	X

Rights concerning IT vendors

For more details, see "Managing IT Vendors", page 47.

	IT RM functional administrator	IT GRC Manager
Establishes the inventories for vendors and publishers See "Vendor Inventory", page 32.	X	
Specifies the annual amount of purchasing See "Specifying the Cost of Products and Services", page 47.	X	X
Assesses the vendors (attributes a score) See "Assessing Vendors", page 48.	X	X

INTERFACE PRESENTATION

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

☛ *For more details on profiles, see "HOPEX IT Risk Management Solution Profiles", page 10 and "Summary of Rights by Profile", page 12.*

The navigation tabs available at the top of the page relate to the different phases of IT risk management:

- **Inventories**
  See "Managing inventories", page 17.
- **Campaign Management**
  See "Assessments by Questionnaires", page 49.
- **Remediation**
  See "Treating risks", page 71.
- **Reports**
  See "HOPEX IT Risk Management Reports", page 81.

Use the **Home** tab to access the objects for which you are responsible.

The Dashboard contains widgets used to access a summary of the information in the repository. For more details, see "Accessing widgets", page 82.

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

ABOUT THIS GUIDE

This guide presents the features of **HOPEX IT Risk Management** solution. It follows these main steps:

- Establishes the IT asset inventory
- Defines the threats and vulnerabilities
- Identifies risks
- Assesses risks
- Remediates Risks
- Generates reports

> ☛ *Reporting functions are available at all times, either globally or for each internal procedural step.*

Guide Structure

This guide comprises the following chapters:

✓ "Defining the Environment for Solutions", page 463: describes the different elements of the environment used in **MEGA** solutions.

✓ "Managing inventories", page 17 describes the inventory of IT assets, threats and vulnerabilities, risks and controls, and vendors.

✓ "Using HOPEX IT Risk Management", page 35 describes the use cases of the solution, that is, how to manage IT risks, compliance and vendors.

✓ "Assessments by Questionnaires", page 49 describes the steps required to send questionnaires when conducting assessment campaigns.

✓ "Treating risks", page 71, describes how to remediate risks and manage action plans.

✓ "Glossary", page 111

✓ "Appendix - Workflows", page 117

Additional Resources

This guide is supplemented by:

- the **HOPEX Common Features** guide, which describes the MEGA interface.

  > ☛ *It can be useful to consult this guide for a more detailed general presentation of the interface.*

- the **HOPEX Power Supervisor** administration guide.

MANAGING INVENTORIES

The IT RM (IT Risk Management) inventories are used to build and view the inventory of the elements necessary to manage risks, compliance and IT vendors.

☛ *For more details on inventory use cases, see "Using HOPEX IT Risk Management", page 35.*

INVENTORY OF IT ASSETS

About the IT Asset Inventory

An IT Asset is company-owned information, system or hardware that is used in the course of its business activities.

There are two "families" of IT assets:

- IT asset (type)

  ☛ *An IT asset type is a specific kind of IT asset regrouping object types (Application, Software technology), as opposed to deployed objects (instances).*

- IT asset (instance)

  ☛ *An IT asset instance is a specific kind of IT Asset regrouping the deployment objects (software installation or deployed technology).*

Importance of the IT Asset Inventory

The first step in managing IT assets is to identify and define the IT assets of your enterprise. You cannot control and manage these assets efficiently until they have been identified.

IT management is essential both in financial and operational terms. In fact, good management leads to optimization of resources, and limits risks linked to compliance and security.

IT asset types

An asset type is a category of assets containing object types (Applications, Software, Technologies), as opposed to deployed objects that are called instances.

We distinguish between:

- Assets
  - Applications

    ☛ *A business application is a set of software tools that make up a consistent whole from a software development viewpoint and with respect to functionalities supplied to users.*

  - Technology

    ☛ *A software technology is a basic component necessary for operation of business applications.*

- Deployed assets:
  - Software installation

    ☛ *A software installation is the deployment of an application with a view to using it on a given site.*

  - Deployed technology

Accessing the IT Inventory

To access the enterprise IT inventory:

- From the main navigation menu, click **Inventories**.

See:

- "Describing Applications", page 19
- "Describing Technologies", page 21
- "Inventory for Threats and Vulnerabilities", page 23
- "Inventory of Risks and Controls", page 28
- "Inventory of Requirements and Regulations", page 31
- "Vendor Inventory", page 32

Describing Applications

To access characteristics that enable identification of an application:

- In the properties pages of an application, select **Characteristics**.

General characteristics of the application

You can specify:

- application **Name**
- the internal **Code**

Type of application

Technologies can be of the following types:

- Office system
- In House Application
- Middleware
- Office System
- System

Functional scope of the application

To view the objects that define the functional coverage of an application:

- In the application properties pages, select **Characteristics** then **Functional Scope**.

The types of data that define functional coverage of the application are:

- The business lines that use the application

> *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.

- The business processes that use the application

  📖 *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.*

- The business capabilities covered by the application

  📖 *A business capability is a component of information system processing. Processing can for example correspond to an activity or an enterprise business.*

Responsibilities concerning an application

Local application owner

An application owner is responsible for managing the application throughout its lifecycle. The application owner ensures that the application is correctly defined.

☛ *The term "owner" identifies a person or an entity who has accepted responsibility for creating, maintaining and using assets. This term does not mean that the person that person has, strictly speaking, ownership rights over the asset.*

To specify one or more owners:

1. In the properties page of the application, expand the **Responsibilities** section.
2. Select the **Local Application Owner** and connect one or more users.

Local IT Risk Manager

The "Local IT Risk Manager" is the local contact for risk at the application level.

☛ *The applications that are linked to a Local IT Risk Manager local or local application owner appear in the **Home** navigation tab, in **To-Do list > My Responsibilities > My IT Assets**.*

Technologies linked to applications

In the properties page of an application, you can connect existing technologies or create new technologies.

To access technologies from an application:

- In the properties page of an application, expand the **Technologies** section.

Data exchanged

This information is derived from **HOPEX IT Portfolio Management**.

Flows, their direction and their content exchanged between applications can be defined. This information enables creation of exchange mapping.

> 🕮 *A message flow is information flowing within an enterprise or exchanged between the enterprise and its business environment. A message flow can carry a content.*

Business data represents the content of a flow.

> 🕮 *A business data indicates content of a message flow. A Business data can be used by several message flows, since it is not associated with a sender and a destination. The same business data can be used by several message flows.*

Vulnerabilities of an application

To view the vulnerabilities of an application:

- In the application properties page, select the **IT Risks** page then expand the **Vulnerabilities** section.

Controls connected to an application

To view the controls for an application:

- In the application properties page, select the **Controls** page.

Describing Technologies

> 🕮 *A technology is a definition or format that has been approved by a standards organization, or is accepted as a standard by the industry.*

Accessing technologies

To access the list of all technologies:

1. See "Accessing the IT Inventory", page 19.
2. Click **Asset Inventory List > All Technologies**.

Defining Technology Characteristics

To specify technical characteristics of a technology:

- In the properties pages of an application, select **Characteristics**, then **Technology**.

You can specify the **Identification** of the technology:

- the **Name** of the technology
- the internal **Code**
- the **Vendor**

Technology types

You can specify the **Technology Type**:

- application services
- operating system
- platform
- RDBMS

A technology can be connected to different technology types.

☛ *Only the functional administrator can create new technology types.*

Risks and vulnerabilities of a technology

You can also connect the technology to:

- risks
- vulnerabilities

📖 *Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset.*

INVENTORY FOR THREATS AND VULNERABILITIES

Examples of Threats, Vulnerability types, and Vulnerabilities

Vulnerability types	Vulnerabilities	Threats
Hardware	Susceptibility to temperature variations	Meteorological phenomenon
Hardware	Unprotected storage	Theft of media or documents
Software	Complicated user interface	Error in use
Network	Poor password management	Unauthorized access
Personnel	Lack of guidelines for software use	Unauthorized use
Site	Location in an area susceptible to flood	Flood

Examples taken from the ISO 27005:2011 standard

Viewing Threats

Threats are external or internal factors that endanger the IT assets of the enterprise. Each threat contains a set of vulnerabilities. For more details, see "Viewing Vulnerabilities", page 24.

Accessing threats

To access threats:

1. See "Accessing the IT Inventory", page 19.
2. Click **Inventories > Threats and Vulnerabilities > All Threats**.

☛ *You can also access threats by threat type. See "Threat characteristics", page 24.*

Creating a threat type

To create a threat type:

1. From the inventory, click **Threats and Vulnerabilities > Threats and Vulnerabilities**.
2. Right-click on the root of the "Threats and Vulnerabilities" tree and select **New > Threat Type**.
   The threat type appears in the tree.

Threat characteristics

You can:

- specify the threat type to which the threat belongs

  📖 *The types of threats are used to organize threats into different categories (e.g.: physical harm, natural events, technical fault, etc.) To create a threat type, see "Creating a threat type", page 23*

- connect vulnerabilities to the threat in the corresponding section.

  ☛ *Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset. For more details, see "Viewing Vulnerabilities", page 24.*

Viewing Vulnerabilities

Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset.

Vulnerabilities can be imported from national databases or managed with appropriate vulnerability management tools.

Accessing vulnerabilities

To access vulnerabilities:

1. See "Accessing the IT Inventory", page 19.
2. From the inventory page, click **Threats and Vulnerabilities > Threats and Vulnerabilities**.

   ☛ *You can also access vulnerabilities by vulnerability type. See "Source", page 25.*

Creating a vulnerability type

To create a vulnerability type:

1. From the inventory page, click **Threats and Vulnerabilities > Vulnerabilities by Vulnerability Type**.
2. Right-click on the root of the "Threats and Vulnerabilities" tree and select **New > Vulnerability Type**.
   The vulnerability type appears in the tree.

Characteristics of vulnerabilities

Threat

A threat can potentially exploit a vulnerability.

☛ *A vulnerability can only be associated with a single threat.*

Type of vulnerability

Vulnerability types organize vulnerabilities into different categories (e.g.: Software, Organization, Site-Location, etc.).

> ☛ *To create a type of vulnerability, see "Creating a vulnerability type", page 24.*

Original release date

The release date is the date at which a vulnerability was described for the first time.

This characteristic is optional. It can be useful when importing from a third-party source.

Last modification date

The last date of modification is the date at which the vulnerability was modified.

This characteristic is optional. It can be useful when importing from a third-party source.

Source

Vulnerabilities are made available and updated regularly by national and standards organizations, for example:

- NIST (National Institute of Standards and Technology)
- CVE (Common Vulnerabilities and Exposures)
- ISO (ISO 27000)

Status

- Potential
- Detected
- Remediated
- Closed

Vulnerability score

- Low
- Medium
- High

Scope of vulnerabilities

The scope of vulnerabilities is made up of two sections:

- assets
- deployed assets

> ☛ *In practice, either one or the other is used, according to the inventory (deployment types)*
>
> ☛ *See "Positioning Vulnerabilities on IT Assets", page 36.*

Vulnerable IT assets

- Applications

  📖 *A business application is a set of software tools that make up a consistent whole from a software development viewpoint and with respect to functionalities supplied to users.*

- Software technology

  📖 *A software technology is a basic component necessary for operation of business applications.*

Vulnerable deployed IT assets

- Software installation

  📖 *A software installation is the deployment of an application with a view to using it on a given site.*

- Deployed technology

  📖 *A software technology is a basic component necessary for operation of business applications.*

CVSS assessment

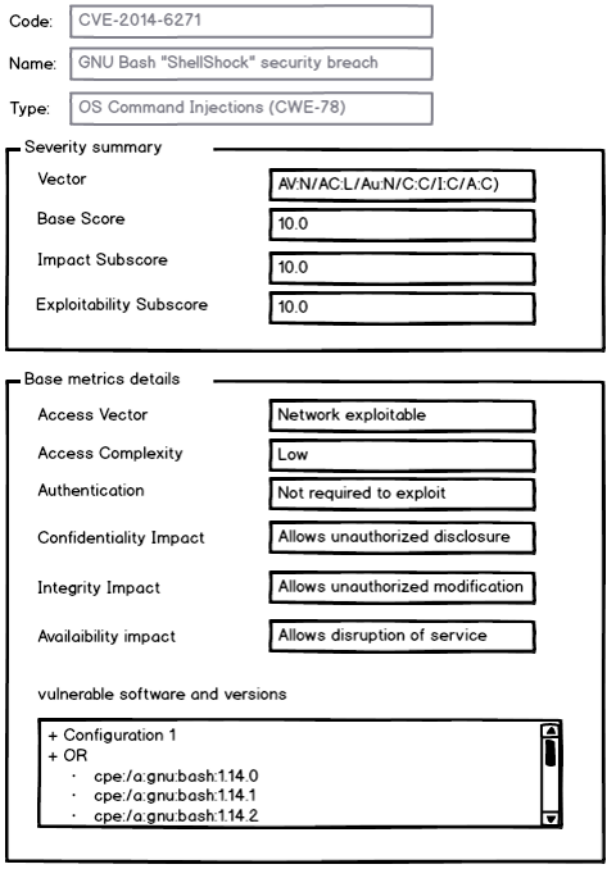
The Common Vulnerability Scoring System (CVSS) is a standardized assessment system for the criticality of vulnerabilities according to objective and measurable criteria.

CVSS is a scoring system enacted by the National Institute of Standards and Technology (NIST) in the United States and is a de facto standard.

☛ *This data is imported using third-party tools and is not entered in **HOPEX IT Risk Management**.*

Examples of data

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6461



Reports concerning vulnerabilities

A number of different reports describe vulnerabilities. See "Reports Concerning Vulnerabilities", page 92.

INVENTORY OF RISKS AND CONTROLS

Viewing Risks

Accessing risks

To access risks:

1. See "Accessing the IT Inventory", page 19.
2. Click **Risks > All Risks**.

You can also access:

- key risks

  ☛ *Key risks are the risks for which the Key Risk check box was selected in the risk properties page.*

- risks not connected to a control.

Assessed characteristics

Impact

The impact characterizes the impact of the risk when it occurs.

Likelihood

The likelihood characterizes probability that the risk will occur.

Inherent risk

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

In summary, an inherent risk = impact x likelihood

Velocity

Velocity represents the rapidity of propogation of the risk of an asset to other assets if an incident occurs. Velocity represent a way to characterize the risk (other than by impact and frequency).

Weighted inherent risk

Inherent risk x velocity

Risk scope

In the risk properties window, you can identify:

- the IT assets at risk
  - applications

    A business application is a set of software tools that make up a consistent whole from a software development viewpoint and with respect to functionalities supplied to users.
  - software technologies

    A software technology is a basic component necessary for operation of business applications.
- deployed assets at risk
  - software installations

    A software installation is the deployment of an application with a view to using it on a given site.
  - deployed technologies

    A software technology is a basic component necessary for operation of business applications.

To specify the risk scope:

1. In the risk properties page, expand the following section as needed:
   - **Scope (IT assets)**, or
   - **Scope (Deployed IT assets)**

     The choice of scope definition has a direct impact on the direct assessments.
2. Connect the objects as you see appropriate.

   For more details on the risk scope, see "Risk scope", page 472

Risk Analysis

For more details, see "Risk analysis", page 472.

Risk assessment

You can assess risks by:

- application
- deployed application (or installation)

  The tab available in the risk properties page depends on the choice made concerning risk assessment.

For more details, see "Direct Risk Assessment", page 41.

Risk treatment

For more details, see "Specifying Controls to be Implemented", page 73.

Viewing Controls

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

It should be noted that a poorly implemented control can represent a vulnerability.

Accessing controls

To access controls:

1. See "Accessing the IT Inventory", page 19.
2. Click **Controls > All Controls**.

You can connect controls in the properties page for a control type.

Scope of a control

You can connect a number of object types to a control with **HOPEX IT Risk Management.**

You can connect:

- the object types present in the standard scope of a control: see "Control scope", page 476
- applications (**Scope (IT Assets)** section).

Control assessment

The **Assessment** tab in the control properties window is used to perform a direct assessment using the "Assessment of controls by application" assessment template.

See "Direct Control Assessment", page 45.

Preparing the Working Environment for Questionnaires

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

- connected risks/controls to applications

  ☛ *For more details, see "Identifying and Positioning Risks", page 37.*

  ☛ *With a view to obtaining pertinent reports, it can be useful to connect the applications to processes, business lines or business capabilities. This is, however, not required to launch assessment campaigns.*

- defined a local application owner for each application

  ☛ *For more details, see "Responsibilities concerning an application", page 20.*

For more details on assessments, see "Assessments by Questionnaires", page 49.

INVENTORY OF REQUIREMENTS AND REGULATIONS

Accessing Requirements and Regulations

To access requirements and regulations:

1. See "Accessing the IT Inventory", page 19.
2. Click **Regulations and Requirements.**
   The regulations and requirements tree appears.

Characteristics of regulations

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

For more details, see "Regulation Characteristics", page 477.

In the regulations page, you can connect:

- business processes (in the **Scope** section)
- sub-regulations
- requirements

Requirement Characteristics

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

For more details, see "Requirement Characteristics", page 479.

To specify the parameter for a requirement:

❱ In the requirement properties, select the **Scope** page.
In the **Contributing Elements** page, you can specify:

- **Control Types**

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

- **Controls**

VENDOR INVENTORY

IT vendors can be software publishers or service providers.

Accessing the list of vendors

To access the list of vendors:

1. See "Accessing the IT Inventory", page 19.
2. Click **Vendors**.

Characteristics of vendors

Vendor type

A vendor is a "Vendor" type entity.

Financial information

See "Specifying the Cost of Products and Services", page 47.

Billing information

- Vendor Corporate Name
- Vendor Doing Business As: (DBA)
- Vendor Billing Address
- Telephone

Main contact information

- Name
- Address
- Email
- Title: Position (for example: Account Manager)

List of technologies provided

In the vendor window, you can view the list of technologies this vendor provides.

Vendor Risk Assessment

In this tab you can allocate a score to the supplier. For more details, see "Assessing Vendors", page 48.

The assessment questionnaires used to assess the vendor also appear here.

USING HOPEX IT RISK MANAGEMENT

Once the IT asset library is built, you can use **HOPEX IT Risk Management** to manage IT risks. You can also use this solution to manage IT compliance and technology vendors.

MANAGING IT RISKS

Once you have established an inventory of the IT assets of your enterprise, you can:

- position vulnerabilities on IT assets
- identify the risks
- position risks on IT Assets
- identify risk scenarios
- assess risks directly or via assessment campaigns
- define action plans for improvement purposes

For more details on the characteristics of risks, see "Viewing Risks", page 28.

You can also, at any time, produce reports on the management of IT risks, threats and vulnerabilities. For more details, see "IT Risk Reports", page 84.

Describing the IT Asset Inventory and Identifying Vulnerabilities

Identifying IT Assets

For you to be able to manage risks, assets must be clearly identified and an inventory of all assets must be established and managed.

☛ *For more details, see "Inventory of IT Assets", page 18.*

Positioning Vulnerabilities on IT Assets

You can identify vulnerabilities and position them on assets (applications and software technologies). You can use a matrix to assist you in this task.

☛ *For more information on vulnerabilities, see "Inventory for Threats and Vulnerabilities", page 23.*

To position vulnerabilities on IT assets:

1. See "Accessing the IT Inventory", page 19.
2. Click **Threats and Vulnerabilities > IT Asset Contextualization**.
3. Click **New**.
4. Click **Add Row** to add vulnerabilities.
5. Click **Add Column** to add IT assets.
6. Click in the cells in question to connect vulnerabilities and IT assets.

☛ *To access application vulnerabilities, see "Vulnerabilities of an application", page 21.*

Identifying and Positioning Risks

To determine the risks to which IT assets are subject, you can:

- use the vulnerabilities identified in the properties page for this asset.

  ☛ *For more details, see "Vulnerabilities of an application", page 21.*

- use the vulnerabilities connected to threats.

  ☛ *For more details, see "Viewing Threats", page 23.*

Once the risks are identified, **HOPEX IT Risk Management** provides two methods for positioning risks on IT assets.

Positioning Risks Using a Matrix

To position risks on IT assets, you can use a specific matrix.

To use the Risks x IT assets matrix:

1. Click on **Library > Risks > Matrix > Risks per IT Asset**.
2. Add:
   - risks in rows
   - IT assets in columns
3. Click in the cells in question to connect vulnerabilities and IT assets.

Positioning risks individually for each asset

Risks can be positioned directly on the IT assets:

- applications
- technologies

Depending on the assessment used, you can choose to position the risks on:

- applications
- applications deployed

For more details, see "Risk scope", page 29.

☛ *Please note that the choice of risk positioning has an impact within the framework of risk assessment. Two different assessment models are available. See "Risk Assessment Templates", page 42.*

Identifying Risk Scenarios

If required, you can define risk scenarios and identify the cause-and-effect relationship between risks.

📖 *An IT risk scenario is the description of an IT event that, if it occurs, can have an impact on the activity of the enterprise.*

Creating a risk scenario

To create a risk scenario:

1. See "Accessing the IT Inventory", page 19.

2. Click **Risks > Risk Scenarios**.
3. Click **New** then **Next**.
4. In the **Risk Scenario Element** section, connect:
   - applications, or
   - software technologies

☛ *The **Risks** section does not display risks that are derived from diagram initialization.*

Creating a risk scenario diagram

The IT RM Manager identifies cause/consequence type dependencies between risks using a risk scenario diagram. This diagram is used to create a network of risks with the aim of identifying pivot risks.

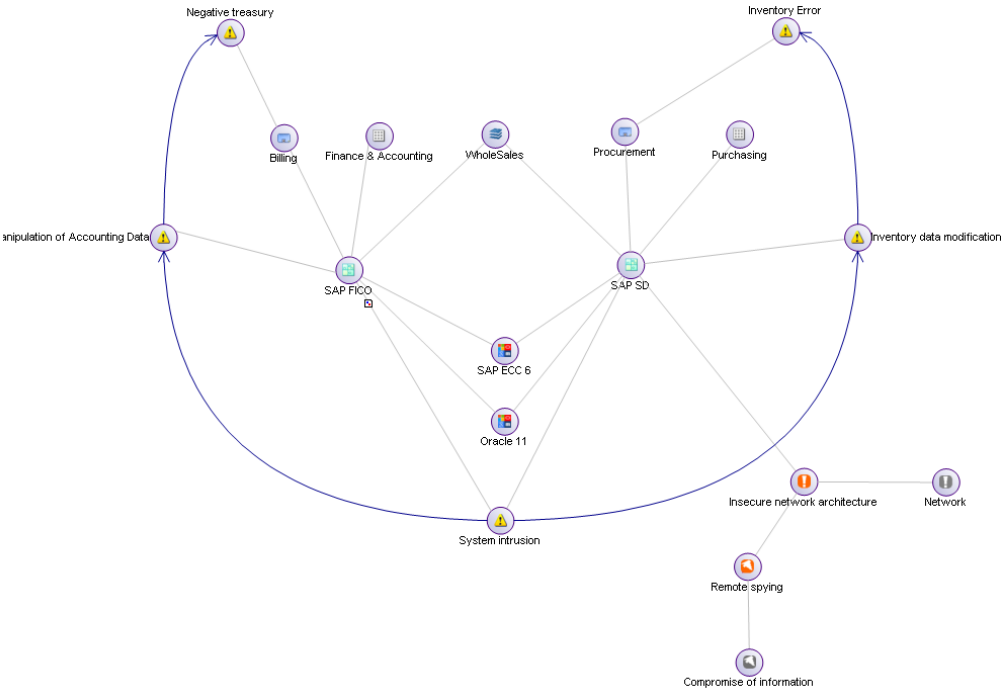
☛ *For more details on pivot risks, see "Pivot risks, causes and consequences", page 39.*

To create a risk scenario diagram:

❱ Click on the risk scenario icon and select **New > Risk Scenario Diagram**.

The following objects are automatically positioned on the diagram:

- the applications or software technologies
- the vulnerabilities and threats
- The business capability processes and business roles are now connected to the application.
- the associated risks



Risk scenario diagram example

Causality links

Risks are linked to each other by causalities (represented by links). These causality links are specific to a scenario.

Pivot risks, causes and consequences

Risks can be considered alternatively as:

- cause
- consequence
- pivot risk

A pivot risk is a risk that, in a risk scenario diagram, is linked to at least one cause and possibly one or more consequences.

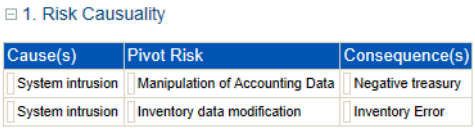
☛ *A pivot risk can have more than one cause and consequence.*

Risk causality report

A risk causality report summarizes the causality links of a risk scenario diagram.

To access this report:

- In the properties page for a risk scenario, select the **Risk Causality Report** page.


1. Risk Causuality

Cause(s)	Pivot Risk	Consequence(s)
System intrusion	Manipulation of Accounting Data	Negative treasury
System intrusion	Inventory data modification	Inventory Error

Risk causality example

This report highlights the "pivot risks" of a risk scenario, that is, risks that are found in the middle of a risk chain.

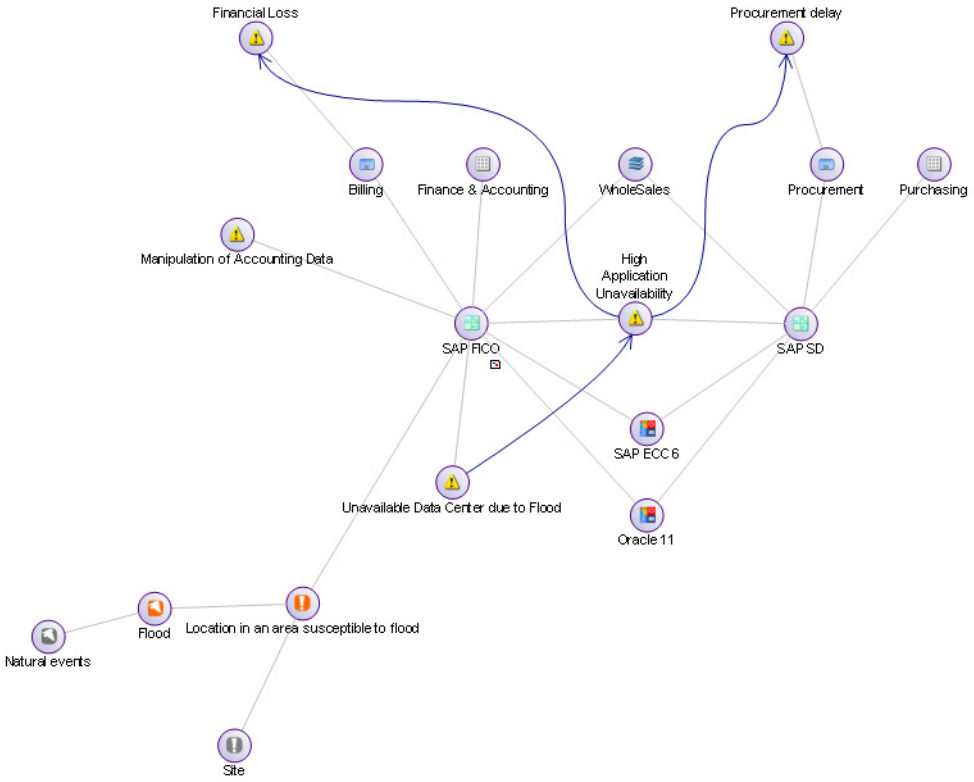
This risk chain comprises:

- risks that are seemingly minor (such as technical IT risks, for example)
- risks that could have major consequences (such as important business risks, for example)

The processing of pivot risks is key to preventing these major risks from arising.

Examples

The scenario diagram below is illustrated by the corresponding causality report.



Cause	Pivot Risk	Consequence
Unavailable date center due to Flood	High application unavailability	Procurement delay
		Financial Loss

Direct Risk Assessment

HOPEX IT Risk Managementis used to directly assess risk level:

- by application, or
- by deployed application (to assess the risk of an entity)

> ☛ *Risks can be positioned either on an application or on a deployed application. For more details, see "Risk scope", page 29.*

Assessing risks directly

The 'expert view' assessment can also be referred to as a direct assessment in **HOPEX IT Risk Management** (that is, without defining an assessment campaign by questionnaire).

To assess a risk directly:

1. In a risk property page, select one of the assessment pages as follows:
   - **Assessment by Installation**: used to assess risks per deployed application
   - **Assessment by Application**

     ☛ *Only one of these tabs appears, depending on the choice you made when positioning risks. For more details, see "Identifying and Positioning Risks", page 37.*
2. Click **Evaluate**.
3. If required, select a context object then select a value for:
   - impact

     🕮 *The impact characterizes the impact of the risk when it occurs.*
   - likelihood

     🕮 *The likelihood characterizes probability that the risk will occur.*
   - velocity

     🕮 *Velocity represents the rapidity of propogation of the risk of an asset to other assets if an incident occurs.*
4. If required, modify the **Measurement Date** and click **OK**.

Risk Assessment Templates

Assessment template	Assessed object	Context	Mode	Assessed characteristics	Assessor
Assessment of risks by application	Risk connected to the application	Application connected to the risk	direct or by campaign	- Impact - Likelihood - Inherent risk - Velocity - Weighted inherent risk	- Direct assessment: IT GRC Manager - By campaign: Application owner
Assessment of risks by deployed application	Risk connected to each deployed application	Deployed application	direct or by campaign	- Impact - Likelihood - Inherent risk - Velocity - Weighted inherent risk	- Direct assessment: IT GRC Manager - By campaign: Application owner

☛ *You can also use these assessment templates for assessment campaigns. For more details, see "Assessments by Questionnaires", page 49.*

Defining Action Plans for Improvement Purposes

The IT RM Manager:

- as the action plan owner, defines the action plans drawn up for improved IT control
- assigns the actions to the application owners responsible for their implementation.

☛ *You can connect action plans to IT assets.*

For more information on action plans, see "Treating risks", page 71.

MANAGING IT COMPLIANCE

Within the framework of managing IT risks, controls are used to ensure compliance.

You can:

- document controls relating to applications managed within the regulatory frameworks in force (example: ISO 2700x).
- connect these controls to the regulatory requirements to be respected.

☛ *For more details on controls, see "Controls", page 474.*

- assess the controls directly or via assessment campaigns.

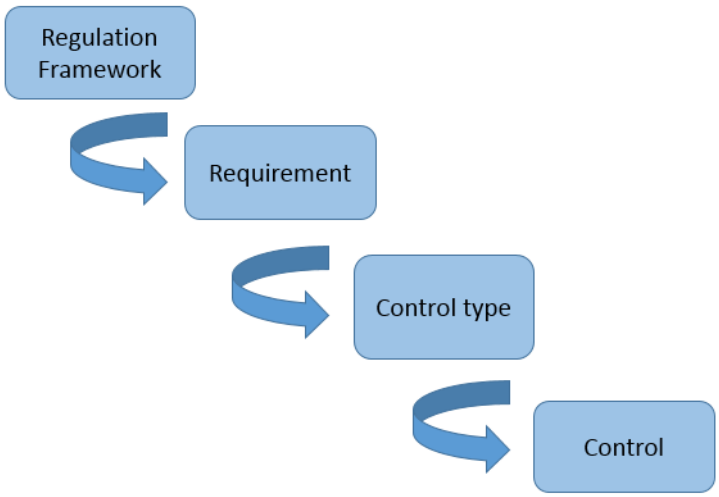
You can, at any time, generate compliance summary reports on the regulation frameworks in force and on the efficiency of the control procedure.

☛ *For more details, see "IT Compliance Reports", page 95.*

Building Controls and Control Type Inventories

Links between controls and control types

To connect a control you must connect it to the matching control type.



Linking control types to regulatory requirements

To connect these controls to the requirements to be complied with:

1. In the property page of a requirement, select the **Scope** tab and expand the **Contributing Elements** section.
2. Connect one or more controls.

Defining the application scope of the control

To define the applications concerned by a control:

1. In the property page of an application, select the **Controls** page and create a control.
2. In the properties page of the control created, expand the **Scope** section and connect **Control Type**.

Defining Regulatory Requirements to be Met

The IT RM Manager defines the regulatory requirements to be complied with for the regulation frameworks in force.

☛ *The regulations, requirements or control types can be imported from a compatible inventory (UCF - Unified Compliance Framework®, for example).*

To access requirements:

- From the inventories page, click **Regulations and Requirements**.

☛ *For more details on regulations and requirements, see "Regulatory Environment", page 477.*

Identifying Controls on Applications

The IT RM Manager identifies the following for each application for which this manager is responsible:

- the regulation frameworks that apply
- the controls, based on predefined controls or controls specifically created

To define the controls for an application:

1. In the application properties page, select the **Controls** page.
2. Create or connect applicable controls.

☛ *You must connect the controls to the applications to proceed with assessments.*

Direct Control Assessment

The IT RM Manager can assess controls directly and thus determine their compliance with regulations. This is an "expert view" assessment.

Assessing controls directly

To directly assess the controls deployed on applications:

1. In the properties of a control, select the **Control Assessment** page.
2. Click the **Evaluate** button.
   The list of applications connected to this control appears.
3. Qualify the **Design** of the control
   - adequate
   - inadequate
4. Qualify the **Effectiveness** of the control
   - effective
   - ineffective
5. If required, modify the **Measurement Date** and click **OK**.

☛ *By default the measure date is today's date. You can select a date earlier than today's date.*

The **Control Level** is automatically calculated from the specified characteristics.

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

☛ *The control level shows "Pass" if the control is considered to be both:*

- *effective*
- *adequate*

Template used to assess controls

Assessment template	Assessed object	Context	Mode	Assessed characteris-tics	Assessor
Assessment of controls by appli-cation	Control	Application connected to the con-trol	direct or by campaign	- Design - Effectiveness	- IT RM Manager (direct) - Control owners (campaigns)

☛ *This assessment model is also used when assessing controls via campaigns.*

MANAGING IT VENDORS

HOPEX IT Risk Management is used to identify IT vendors (software editors and service providers).

You can:

- specify the cost of products and services purchased from each vendor for the past year.
- assess vendors by assigning them a value, based where appropriate on the questionnaires sent via campaigns.

You can, at any time, generate summary reports concerning vendor scores. For more details, see "Vendor Management Reports", page 103.

Identifying IT Vendors

The IT RM functional administrator identifies IT vendors (software editors, service providers).

☛ *For more details on vendors, see "Vendor Inventory", page 32.*

☛ *The vendors and technologies may have previously been identified in **HOPEX IT Portfolio Management** or **HOPEX IT Architecture**.*

Specifying the Cost of Products and Services

Every year, the IT RM Manager enters a global annual amount for products and services purchased from the vendor.

On this basis, the IT GRC Manager determines the rank of the supplier.

☛ *This information is entered for reference purposes in **HOPEX IT Risk Management**.*

To enter these costs:

1. See "Accessing the IT Inventory", page 19.
2. Click **Vendors**.
3. Select a vendor in the list that appears.
4. In the properties of a vendor, select the **Vendor Information** page.
5. In the properties dialog box, enter the following information in the **Financial Information** section:
   - Total amount purchased
   - Rank

   ☛ *The information in this section is for the end of the year prior to the current year.*

You can specify the following information:

- Main contact information
- Billing information

☛ *For more details, see "Vendor Inventory", page 32.*

Assessing Vendors

The IT RM Manager can assess the risk associated with a vendor.

To assess a vendor:

1. See "Accessing the IT Inventory", page 19.
2. Click **Vendors**.
3. Select a vendor in the list that appears.
4. From vendor properties, select the **Vendor Risk Assessment** page.
5. Enter a value to qualify the risk linked to the vendor.

☛ *You can also launch campaigns with a view to assessing the vendor and if required, confirming your assessment. In this case, the assessor must be defined in the assessment session. For more details, see "Assessments by Questionnaires", page 49.*

ASSESSMENTS BY QUESTIONNAIRES

HOPEX enables assessments using standard questionnaires. The assessment questionnaires are sent to appropriate respondents.

This chapter describes the principle of performing assessments using questionnaires.

☛ ***HOPEX*** *solutions are used to perform assessments:*

- *expert view assessments (called direct assessments)*
- *via assessment campaigns using questionnaires sent out as described here.*

PRINCIPLE OF ASSESSMENTS BY CAMPAIGNS

📖 *An assessment is a mechanism used to receive feedback (qualitative or quantitative) from an identified population on identified objects. The assessment is then supplemented by results analysis tools.*

Concepts overview

Assessment session

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

Questionnaire

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

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

Assessment campaign

With **HOPEX** solutions, an assessment session is started in the context of an assessment campaign.

📖 *A campaign enables grouping of several sessions.*

Assessment Steps

Preparing the work environment

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

☛ *For more details, see "Preparing the Working Environment for Questionnaires", page 30.*

Starting a campaign and assessment sessions

See "Steps of assessment workflow with campaign", page 44:

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

- ✓ "Creating Assessment Campaigns", page 52
- ✓ "Creating Assessment Sessions", page 53
- ✓ "Planning Sessions Within a Campaign (Optional)", page 55

> ☛ *Planning the campaign is optional. If you do not deploy the assessment campaign, go directly to "Validating Assessment Campaigns", page 58.*

- ✓ "Validating Assessment Campaigns", page 58
- ✓ "Displaying the Objects to Assess and their Contexts", page 59
- ✓ "Defining the Scope of the Assessment Session and the Respondents", page 60
- ✓ "Validating the Objects to Assess and their Contexts", page 61
- ✓ "Sending Questionnaires", page 63

> ☛ *It is not necessary to manually execute deployment, validation and launch if you choose to launch the assessment session immediately after you created it or if you schedule it from the creation wizard. See "Variations in the Launch of Assessment Sessions", page 21.*

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

- ✓ "Completing Questionnaires", page 64
- ✓ "Monitoring Questionnaire Progress", page 66
- ✓ "Closing the assessment session", page 69

CREATING ASSESSMENT CAMPAIGNS

A campaign enables grouping of several sessions.

You can create an assessment campaign:

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

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

Accessing Assessment Campaigns

To access assessment campaigns:

❱ From the main navigation menu, click **Campaign Management > Campaigns**.

Creating Assessment Campaigns

To create an *assessment* campaign:

1. Select **Campaign Management > Campaigns > Campaigns> Campaigns**.
   The list of campaigns appears in the edit area.
2. Click **New**.
   The campaign creation page appears.
3. In the **Campaign Type** field, select "With Template".
4. Select the appropriate **Assessment Template**.
5. Modify the **Calendar** if required.

   ☛ *The calendar serves to initialize begin and end dates of the assessment campaign.*
6. Specify the **Begin Date** and the **End Date** of the assessment.
7. Click **Suivant** then **OK**.
   The campaign is created.

With assessment models supplied as standard in the **HOPEX IT Risk Management** solution, you can specify the objects to be assessed for an assessment session.

See "Creating Assessment Sessions", page 53.

CREATING ASSESSMENT SESSIONS

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

Accessing Assessment Sessions

To access an assessment session:

1. Click **Campaign Management** and select the assessment campaign in question.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

2. In the properties page of the assessment campaign, select the **Sessions** page.

Creating Assessment Sessions

Creating Assessment Sessions

To create an assessment session:

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

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

   ☛ *You may choose to launch the assessment session now or to schedule it. See "Creating and launching assessment sessions", page 54.*

4. Click the **Save** button.
5. You can create other assessment sessions in the same way.

   ☛ *The assessment sessions created will be used to plan the assessment campaign, that is to distribute between the different assessment sessions the objects to be assessed in their context. See "Distributing Assessments Within Sessions", page 56.*

Previewing assessment session parameters

Once the assessment session is created, you can preview the parameters inherited from the assessment campaign.

> ☛ *To access an assessment session, see "Accessing Assessment Sessions", page 53.*

To preview the parameters:

1. Open the properties of the assessment session and select the **Parameters and Preview** tab.
   Elements that will be assessed appear.
   In particular, you can view:
   - assessed characteristics (defined in the assessment template)

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

     > 🕮 *A context object is an object in the framework of which the assessment is carried out. For example, a risk can be assessed within the framework of an application or a deployed application.*
   - assessment nodes which correspond to objects placed in their context objects, associated with respondents.

     > 🕮 *An assessment node is associated with values calculated from answers given in questionnaires by respondents for each of the assessed characteristics. It is created at the time of deployment of the assessment session, or at aggregation. Objects created at deployment are owned by the session and enable determination of the object that will be evaluated, by whom and in which context.*

Creating and launching assessment sessions

See "Creating Assessment Sessions", page 53.

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

- "**now**"
  If you choose this option, you will be able to see the assessment session being launched. This option enables to execute the following workflow transitions at the same time:
  - deploy: "Displaying the Objects to Assess and their Contexts", page 59
  - validate: "Validating the Objects to Assess and their Contexts", page 61
  - start: "Sending Questionnaires", page 63
- after saving, in batch mode ("**as soon as possible**")
- later, specifying the date and hour in UTC format ("**planned**")

PLANNING SESSIONS WITHIN A CAMPAIGN (OPTIONAL)

This step, which is optional, is useful when you are creating several assessment sessions.

You can go directly to:

- step "Creating Assessment Sessions", page 53:
- step "Validating Assessment Campaigns", page 58

You can choose to schedule the assessment sessions during the campaign. If so, you must follow these steps:

- deploying the assessment campaign
- defining the assessment campaign scope
- distributing the assessments among the sessions

Deploying Assessment Campaigns

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

☛ *This step is optional. If you are not deploying the assessment campaign, go directly to "Validating Assessment Campaigns", page 58*

To deploy a campaign:

1. In the list of campaigns, click the icon of the campaign you created and select **Assessment Campaign (In Preparation) > Deploy**.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

2. In the deployment window, indicate that you want to deploy the campaign now.

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

   - *now*
   - *as soon as possible (after dispatch)*
   - *at a later date*

3. Click **OK**.
   Assessment nodes are created.

   📖 *An assessment node comprises:*

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

You can now define assessment campaign scope. See "Defining Assessment Campaign Scope and Respondents", page 56.

Defining Assessment Campaign Scope and Respondents

Having deployed the assessment campaign, you must:

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

☛ *For more details on assessment nodes, see "Deploying Assessment Campaigns", page 55*

Defining assessment campaign scope

To define campaign scope:

1. In the properties of the campaign, select the **Effective Scope** tab.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

   The list of assessment nodes from your deployment appears.
2. Select the values you want to remove from the campaign and click the **Unvalidate** button.

Specifying respondents

To add or modify respondents:

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

Distributing Assessments Within Sessions

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

This consists of distributing assessments during the assessment sessions.

To plan the campaign:

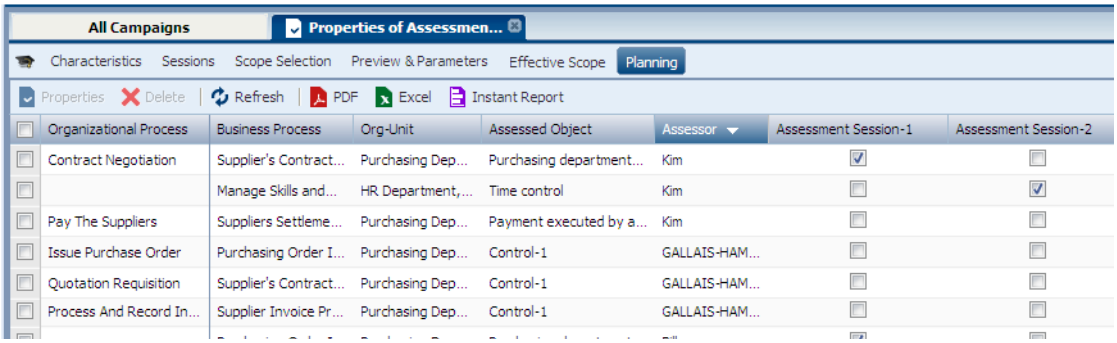
1. In the properties of the assessment campaign, select the **Planning** tab.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

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

2. In the right pane, select the assessment sessions in which you want to assess the object in its context.

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



☛ *Respondents are specified at step "Defining Assessment Campaign Scope and Respondents", page 56.*

VALIDATING ASSESSMENT CAMPAIGNS

You can validate an assessment campaign:

- directly after having created a session, or
- after planning the campaign

> ☛ *For more details, see "Creating Assessment Sessions", page 53 and "Planning Sessions Within a Campaign (Optional)", page 55.*

Validating an assessment campaign freezes its parameters (for example scope or planning).

To validate the campaign:

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

> ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

You can now prepare the start of the assessment session and deploy the assessment session. See "Displaying the Objects to Assess and their Contexts", page 59.

DISPLAYING THE OBJECTS TO ASSESS AND THEIR CONTEXTS

After validating your campaign, you must define the objects to be assessed and their contexts. For this, you must ***deploy the assessment session***.

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

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

The session manager can then review this list.

To create the list of assessment nodes of a session:

1. Open the properties page of the campaign and select the **Session** tab.

   > ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

2. In the **Assessment Session** section, right-click the session that interests you and select **Assessment Session (In Preparation) > Deploy**.

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

   This operation can take several minutes.

DEFINING THE SCOPE OF THE ASSESSMENT SESSION AND THE RESPONDENTS

Having deployed the assessment session, you can:

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

> ☛ *If you have defined the scope on the assessment campaign, you do not necessarily need to redefine it on the assessment session. For more details, see "Defining Assessment Campaign Scope and Respondents", page 56.*

Defining the Session Scope

To access the list of calculated assessment nodes:

❱ Open the properties of the assessment session and select the **Effective Scope** tab.

> ☛ *To access the session, see "Accessing Assessment Sessions", page 53*

You can now select the objects to be assessed in the session.

With this list you can:

- duplicate, validate, invalidate or delete elements to be assessed
- assign them a respondent.

Specifying respondents

To add or modify respondents:

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

> ☛ *To access the session, see "Accessing Assessment Sessions", page 53*

VALIDATING THE OBJECTS TO ASSESS AND THEIR CONTEXTS

Validating an assessment session validates the objects to be assessed in their context as well as their respondents.

The effect of this assessment session validation is to ***generate the questionnaires*** without, however, sending them to addressees.

Validating the Assessment Session

To validate the sessions and generate questionnaires

1. Open the properties page of the campaign and select the **Session** tab.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

2. In the **Assessment Session** section, click the session that interests you, then **Assessment Session > Validate**.
   All questionnaires are created with status "To send". This operation can take several minutes.

You can now view questionnaires that have been generated.

Viewing Generated Questionnaires

To view generated questionnaires:

1. In the properties of an assessment session, select the **Questionnaires** tab.

   ☛ *To access the session, see "Accessing Assessment Sessions", page 53*

2. Select the row relating to the assessment session and click **Display Questionnaires**.
3. Open each of the questionnaires to display the associated assessment nodes and questions.

   ☛ *If questionnaire presentation is unsatisfactory, the functional administrator can modify it at this stage. For more details see the **HOPEX Assessment** guide, "Assessment Template" chapter. In the solution, questionnaire templates are available in the tab concerning campaign management **> Preparation > Questionnaire Templates**.*

   ☛ *At this stage you can still modify presentation of questionnaires.*

   ☛ *It is recommended that the assessment session be validated just before starting the session. If you validate too early, information concerning respondents could be incorrect.*

Regenerating Questionnaires

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

To regenerate questionnaires:

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

  ☛ *To access the session, see "Accessing Assessment Sessions", page 53*

SENDING QUESTIONNAIRES

After validating the assessment session, you can ***start the assessment session***, which sends the questionnaire to the respondents.

To start the assessment session:

1. Select **Assessment Campaigns > Campaigns > Campaigns**.
   The list of campaigns appears in the navigation tree.
2. Select the campaign that interests you and click **Properties**.
   Properties of the campaign appear in the edit area.
3. In the **Sessions** section, click the session that interests you, then **Assessment Session > Start**.
   The session activation page appears.
4. Click the **Save** button at top of the page.
   The *assessment questionnaires* are sent to respondents defined in the assessment session perimeter.

COMPLETING QUESTIONNAIRES

The steps described here concern questionnaire respondents.

> ☛ *For more information on the how to process a questionnaire, see the appendix in the section concerning questionnaire workflows.*

Accessing Assessment Questionnaires

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

To complete questionnaires:

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

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

Requesting questionnaire transfer

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

To make a transfer request:

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

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

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

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

MONITORING QUESTIONNAIRE PROGRESS

Consulting Session Results

To consult progress of an assessment session:

- Open the properties of the assessment session and select the **Reports > Follow-Up** tab.

  ☛ *To access the session, see "Accessing Assessment Sessions", page 53*

Viewing Questionnaires Sent

To access the list of questionnaires sent:

- Select **Campaign Management > Campaigns > Follow-Up > Questionnaires Sent**.

Validating Assessment Questionnaires

To access the list of assessment questionnaires completed by respondents:

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

Asking a respondent to modify answers

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

To make a modification request:

1. Select **Campaign Management > Campaigns > Follow-Up > Questionnaires Answered**.

2. Click the icon of a questionnaire and select **Assessment Questionnaire (To Be Validated) > Ask For Modification**.

   ☛ *The respondent can modify his/her answers. See "Completing Questionnaires", page 64.*

Reassigning questionnaires

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

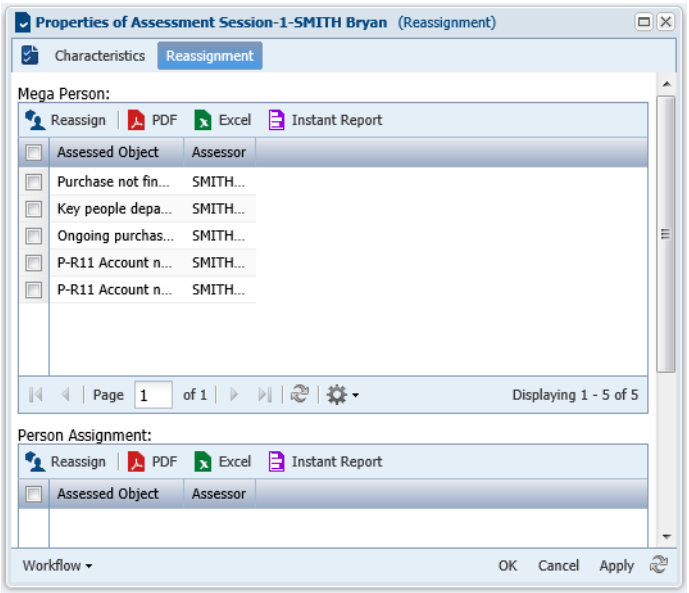
To reassign a questionnaire:

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

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

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

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



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

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

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

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

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

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

CLOSING THE ASSESSMENT SESSION

You can close the session at any time.

To close an assessment session:

1. Open the properties page of the campaign and select the **Session** tab.

   ☛ *To access the campaign, see "Accessing Assessment Campaigns", page 52*

2. In the **Assessment Session** section, right-click the session that interests you and select **Close**.
   All questionnaires are automatically closed. This operation can take several minutes.

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

TREATING RISKS

With a view to ongoing improvement, enterprises must carry out actions to eliminate non-compliance causes with respect to IT requirements to prevent their reoccurrence.

HOPEX IT Risk Management is used to specify, implement and follow up action plans defined for treating risks. Treating risks also consists of selecting and implementing controls aimed at reducing the risk.

The IT RM Manager defines the action plans for controlling IT risks and allocates actions to the application owners responsible for implementing these plans.

✓ "Risk Treatment Mode", page 72
✓ "Managing action plans", page 74

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

RISK TREATMENT MODE

To specify risk treatment choices:

1. In the properties page of a risk, select the **Treatment** tab.

   ☛ *To access risks, see "Accessing risks", page 28.*

Treatment Modes

Various solutions that enable facing the risk are proposed.

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

The different scenarios possible are analyzed to weigh up their positive and negative aspects, with a view to selecting a scenario compatible with the risk control level in question.

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

Risk levels

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

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

Specifying Controls to be Implemented

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

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

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 **Treatment** page 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.

    ☛ *For more details, see "Managing action plans", page 74.*
  - The **Controls** tab lists controls planned for risk reduction.

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

MANAGING ACTION PLANS

Creating Action Plans

To create an action plan:

1. Click the main navigation menu, then **Inventory**.
2. Select **Reports > Remediation > Action Plans**.
3. Click **New**.
   The action plan is created.

You can specify action plan characteristics in its properties. See "Characterizing Action Plans", page 74.

Characterizing Action Plans

To specify action plan properties:

1. Click the main navigation menu, then **Inventory**.
2. Select **Remediation > All Action Plans**.
3. Open the properties of the action plan.

General characteristics

You can specify the following information:

- **Name**: action plan name.
- **Owner**: this field is specified by default by the user who created the action plan.
- **Owner Entity**: entity responsible for action plan implementation.
- **Approver**: user responsible for validation of the action plan when all actions are completed.
- **Means**: text description of means required/desired for action plan execution.
- **Priority**: enables indication of a level. Priority can be:
  - "Low"
  - "Medium"
  - "High"
  - "Critical"
- **Origin**: enables definition of the context of carrying out the action plan:
  - "Audit"
  - "Compliance"
  - "Event"
  - "Risk"
  - "RFC"
  - "Other".
- **Category**: the action plan can for example be connected to:
  - risk impact reduction
  - project management
  - process improvement
  - control performance improvement
  - etc.

    ☛ *Other values are available.*
- **Nature**: enables definition of whether the action plan is:
  - Corrective
  - Preventive
- **Comment**: supplements information on the action plan and its characteristics.
- **Steering Calendar**: used for sending reminders to the person responsible for an action plan so that they can indicate action plan progress.

  ☛ *A steering calendar for monthly reminder of progress is supplied by default.*

Financial assertion

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

RACI

The action plan **Owner** responsible for definition of actions to be carried out and their execution.

This field is specified with the name of the action plan creator or with the name of the action plan approver.

☛ *For more details on the use of RACI, see "Responsibilities", page 30.*

Success factors

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

Scope

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

You can connect objects of the following types:

- Controls
- applications
- risks
- entities
- process
- incidents

Milestones

Milestones are key dates of the action plan.

☛ *The planned end date is mandatory.*

Attachments

You can attach business documents to an action plan:

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

Managing Actions

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

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

To create an action from an action plan:

1. In the main navigation menu, click **To-Do List** then **My Responsibilities > My Action Plans**.

   ☛ *Depending on your profile, you can also access action plans via the menu **Remediation > Action Plans**.*
2. Select the action plan in question and click **Properties**.
3. In the **Actions** section, click **New**.
4. In the action properties, complete fields:
   - **Priority**: enables indication of a level. Priority can be: "Low", "Medium", "High" or "Critical".
   - **Owner**: responsible for the action as specified by the action plan creator.
   - **Owner Entity**: entity responsible for action plan implementation.
5. You can specify milestones, which are important dates of the action.
   - **Planned Begin Date**
   - **Planned End Date**
6. Click **OK**.
   The action is created.

Action Plan Workflows

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

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

☛ *Commands enabling passage from one workflow status to another are available:*

- *in the pop-up menu of the action plan from an action plans list*
- *in the properties dialog box of an action plan, by clicking the action plan icon at top left*

"Bottom-up" approach

In a "bottom-up" approach, the action plan can be created by any user (for example, the Application owner or the IT RM Manager. An approver must validate the action plan so that it can be implemented. This is the case when assessment questionnaire respondents propose an action plan: they must first submit it via the workflow.

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

"Top-down" approach

In the framework of a "top-down" approach, the action plan is created by a responsible. The action plan does not need to be validated in this case.

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

Action workflow

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

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

☛ *See "Action Workflow", page 145.*

Action Plan Follow-Up

Indicating action plan progress

You can create progress states to indicate its progress.

To specify action plan progress:

1. From the navigation menu, select **Remediation > Action Plans**.
2. Select an action plan and open its properties.
3. Expand section **Action Plan Progress**, and in the **Progress Update** frame, click **New**.
4. Specify a **Progress Update Percentage**.
5. If required, specify the **Progress Assessment**.
   You can specify if the action plan is:
   - On Time
   - Delayed
6. Click **OK**.
   The progress state is created. You can create these at regular intervals.

Action plan follow-up reports

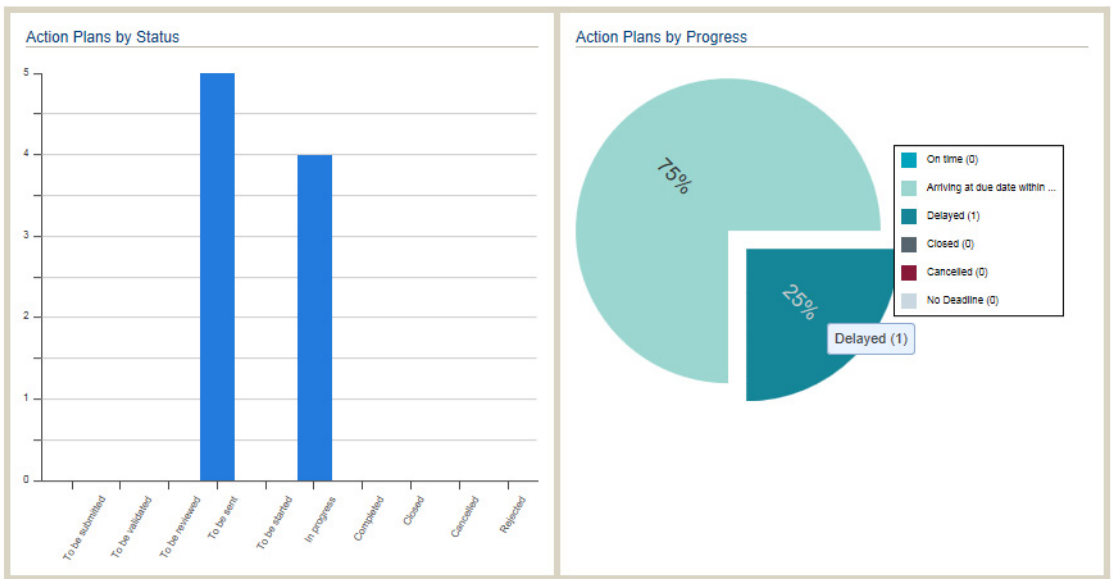
You can follow up on action plans with reports.

To access the Reports tab:

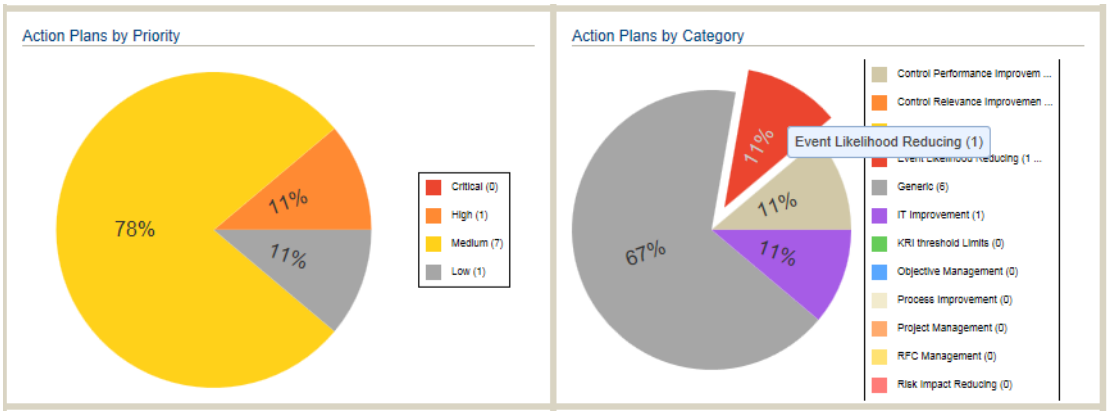
1. From the navigation menu, select **Remediation > Action Plans > Follow-up Report**.
2. Click **New**.

☛ *You can, if necessary, specify parameters in the corresponding tab.*

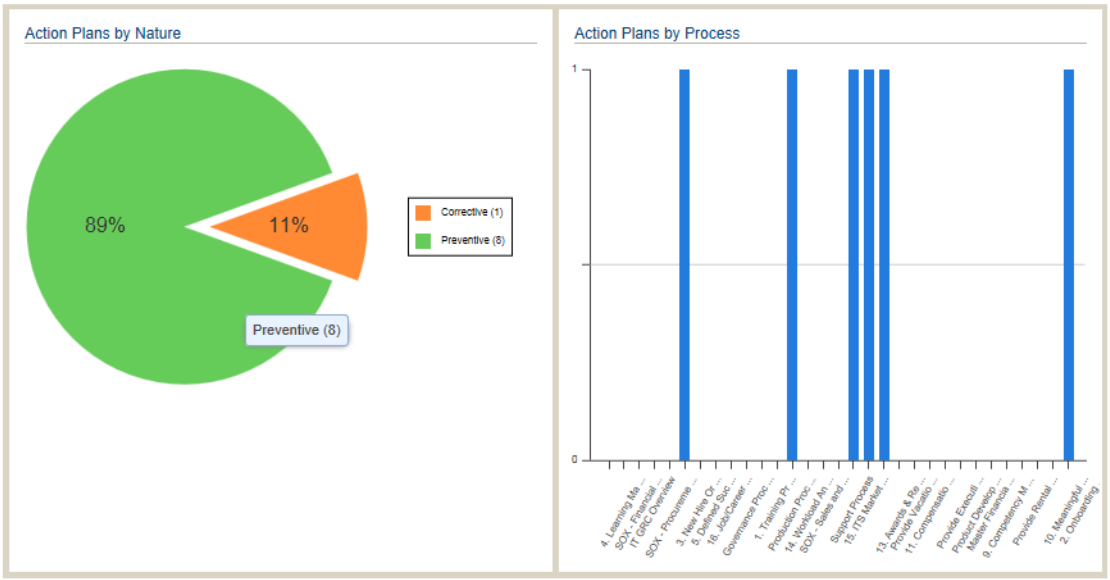
3. Click the **Reports** tab to display the results.
   This report contains a number of bar and pie charts represent the distribution of action plans
   - by status
   - by progress



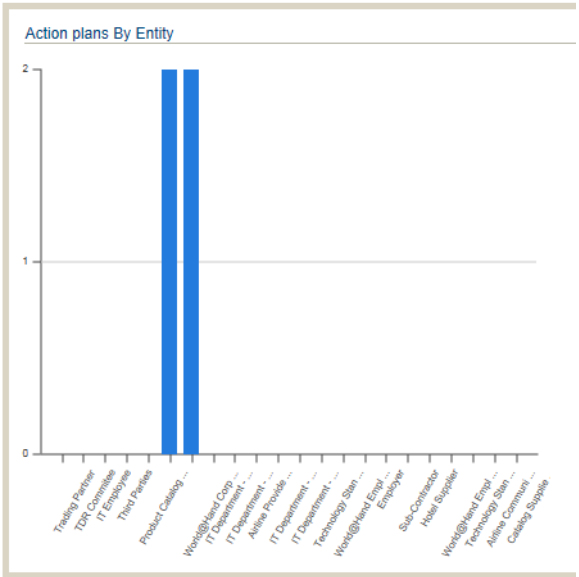
   - by priority
   - by category



- by nature
- by process



- by entity



To access the action plans concerned:

1. Click in the bar or the pie chart sector in question.
2. The corresponding actions plans appear in a list on the bottom of the page.

HOPEX IT Risk Management Reports

This chapter describes the reports used in **HOPEX IT Risk Management**.

Report results can differ according to the assessment template of the selected assessment.

☛ *To customize reports, see **HOPEX Common Features** guide, "Generating Documentation", "Customizing Reports".*

ACCESSING REPORTS

There are a number of different ways to access reports in **HOPEX IT Risk Management**.

Accessing the report tab

A large number of reports are available in the Reports tab.

To access the Reports tab:

1. Open the **HOPEX IT Risk Management** desktop.
2. From the main navigation menu, click **Reporting**.
   Reports are classified by theme:
   - "IT Risk Reports", page 84
   - "IT Compliance Reports", page 95
   - "Vendor Management Reports", page 103

Accessing reports directly available on objects

In addition to the reports listed in the Reports tab, reports are available:

- directly on objects
- in the solution menus, in particular in the form of matrices that are also used to modify the repository

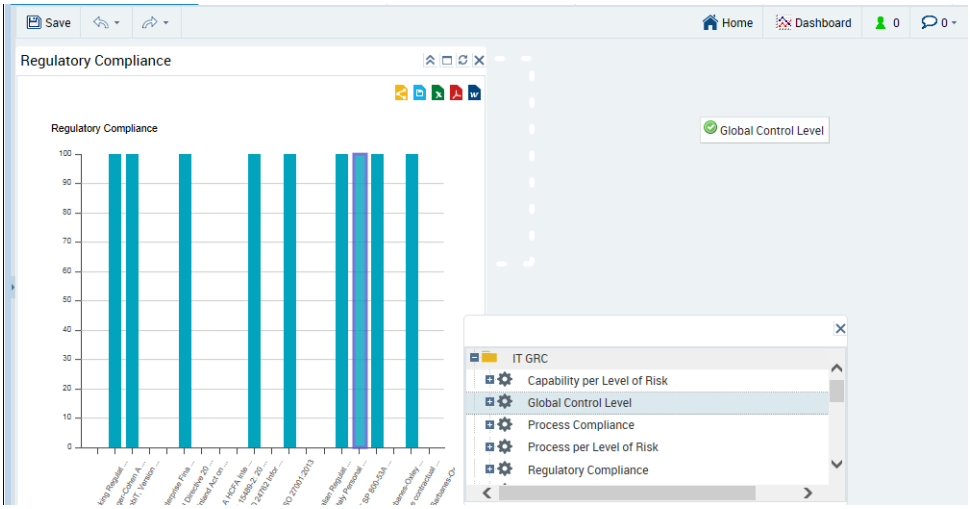
Accessing widgets

You can easily add widgets to your dashboard.

To add a widget:

1. From the main navigation menu, click **Dashboards**. In the lower left of the edit area, click **Add**.

2. In the window that appears, select the widget that you want to add and drag-and-drop it on your desktop.



IT Risk Reports

☛ *For more details on risk management, see "Managing IT Risks", page 36.*

Risk Identification Reports

Criticality of applications

Access path

Reports > IT Risk > Identification > Application Criticality

Parameters

- Business process: list of 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.*

- Type of application (optional)

Result

This report presents, in bubble form, the applications connected to business processes, with the following information:

X-axis	The number of applications interfaced via application flows with the application in question
Y-axis	The number of business capabilities connected to the application
Size of the bubble	Number of software installations for the application
Color of the bubble	Depends on the global cost of the application

📖 *A business capability is a component of information system processing. Processing can for example correspond to an activity or an enterprise business.*

☛ *The global cost of the application is available in **HOPEX IT Portfolio Management**.*

Example

Table of Threats and Vulnerabilities

Access path

Reports > IT Risk > Identification > Threat and Vulnerability Table

Parameters

- Start and end dates

  ☛ *The start and end dates define the value range to take into account for the assessments. If the same object is assessed more than once during this period, the most recent assessment is taken into account.*

- Threats using vulnerabilities

  Threats are external or internal factors that endanger the IT assets of the enterprise.

  Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset.

Result

The report presents the risks via the Threat > Vulnerability > Application tree.

It displays the most recent risk assessment for the application context.

Example

Threat	Vulnerability	Vulnerability Type	IT Asset	Risk	Impact	Inherent Risk	Likelihood	Velocity	Weighted Inherent Risk
Remote spying	Insecure network architecture	Network	SAP FICO	Manipulation of Accounting Data					
Remote spying	Insecure network architecture	Network	SAP FICO	High Application Unavailability	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP FICO	Unavailable Data Center due to Flood					
Remote spying	Insecure network architecture	Network	SAP FICO	System intrusion	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP SD	High Application Unavailability	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP SD	Inventory data modification					
Remote spying	Insecure network architecture	Network	SAP SD	System intrusion	Very Low	Very Low	Rare	Very Low	Very Low

IT Asset Reports

Risk level aggregated by business process

Access path

Reports > IT Risk > IT Assets > Aggregated Risk Level per Business Process

Parameters

- Start and end dates

  ☛ *The start and end dates define the value range to take into account for the assessments. If the same object is assessed more than once during this period, the most recent assessment is taken into account.*

- Assessment template:
  - for applications
  - for installations

  ☛ *For more details on assessment templates, see "Risk Assessment Templates", page 42*

- Business process

  ☛ *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.

The **Generate Aggregation** button starts the calculation and consolidates the risk assessments on the applications and processes.

Result

This report is presented in the form of a Business Process > Application > Risks tree.

The assessment result appears for each element in the tree.

Example

	Impact	Likelihood	Inherent Risk	Velocity	Weighted Inherent Risk
P1	Medium	Likely	Medium	Medium	Medium
A2	High	Likely	High	Medium	High
R1	High	Likely	High	Medium	High
A1	Low	Possible	Medium	Medium	Medium
R3	Medium	Likely	Medium	Medium	Medium
R1	Very Low	Rare	Very Low	Very Low	Very Low
R2	Low	Possible	Low	High	Medium
P2	High	Likely	High	Medium	High
A2	High	Likely	High	Medium	High
R1	High	Likely	High	Medium	High

Risk Heatmap

Access path

Reports > IT Risk > IT Assets > Heatmap of Risks

Parameters

- Begin and end date

  ☛ *These dates define the value range to take into account for the assessments. If the same object is assessed more than once during this period, the most recent assessment is taken into account.*

- Risks: used to select the risks by filtering them according to a number of criteria.

You can select the risks to be taken into account using the trees.

Risk selection criterion	Corresponding selection tree
Business line	Business line > Applications > Risks
Risk type	Risk types > Risks

Risk selection criterion	Corresponding selection tree
Business	Process > Applications > Risks
Business capability	Business capabilities > Applications > Risks
Threats	Threats > Vulnerabilities > Applications > Risks

Result

Heatmaps illustrate the following characteristics:

- Impact / Likelihood

  📖 *The impact characterizes the impact of the risk when it occurs.*

  📖 *The likelihood characterizes probability that the risk will occur.*

- Inherent risk / Velocity

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

  📖 *Velocity represents the rapidity of propogation of the risk of an asset to other assets if an incident occurs.*

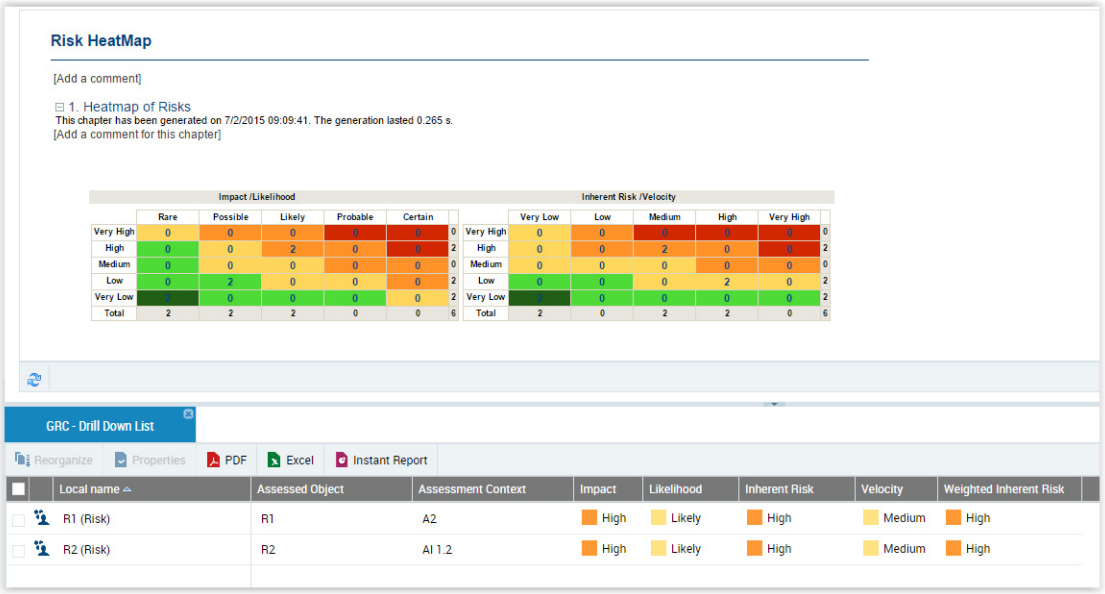
The values in each cell represent the risk assessments selected.

☛ *By default, all risks are taken into account.*

To display the assessments corresponding to each cell:

❱ Click the value of the cell.
The assessments appear with the risk assessed and its context (application or software installation).

Example



Application Heatmap

Access path

Reports > IT Risk > IT Assets > Heatmap of Applications

Parameters

- Begin and end date

  ☛ *The start and end dates define the value range to take into account for the assessments. If the same object is assessed more than once during this period, the most recent assessment is taken into account.*

- Applications: used to select the applications to take into account, based on the criteria and trees.

Application selection criterion	Corresponding selection tree
Business	Processes > Applications
Business line	Business line > Applications
Business capability	Business capabilities > Applications

Result

Heatmaps illustrate the following characteristics:

- Inherent risk / Velocity

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

  Velocity represents the rapidity of propogation of the risk of an asset to other assets if an incident occurs.

- Impact / Likelihood

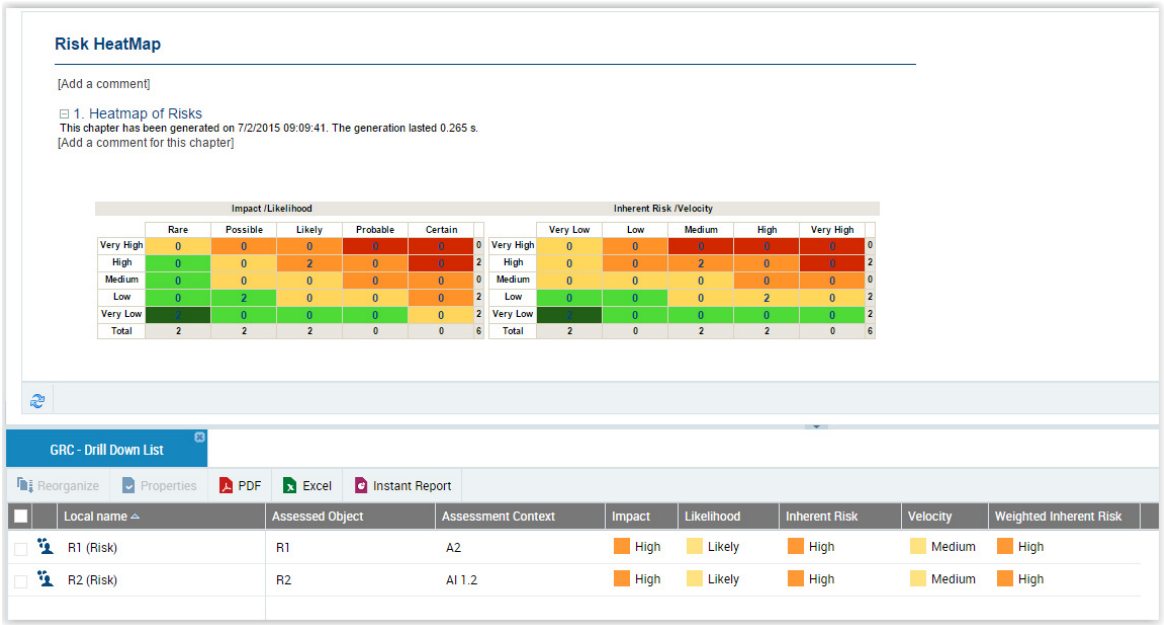
  The impact characterizes the impact of the risk when it occurs.

  The likelihood characterizes probability that the risk will occur.

The values in each cell represent the average risk level of the application.

To display the assessments concerning the applications, click on the value of the cell.

Example



Risk widgets

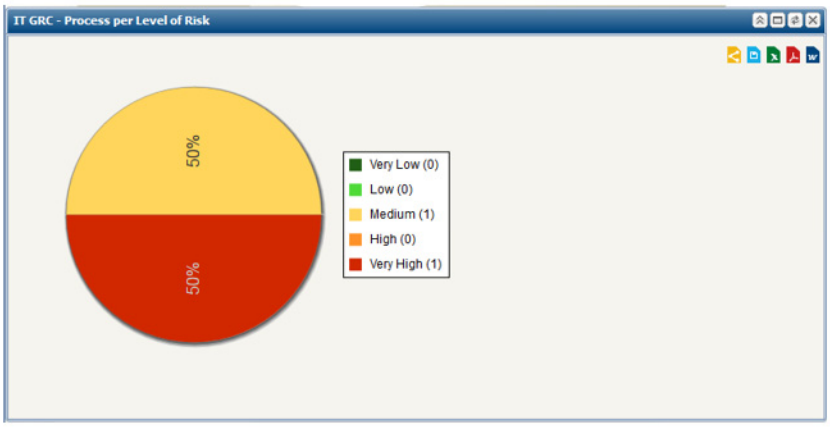
Widgets are accessible from the dashboard via the home page.

They do not contain any parameters.

Process widget by risk level

This widget is used to display the percentage of first-level business processes according to the value of the average inherent risk for the process.

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

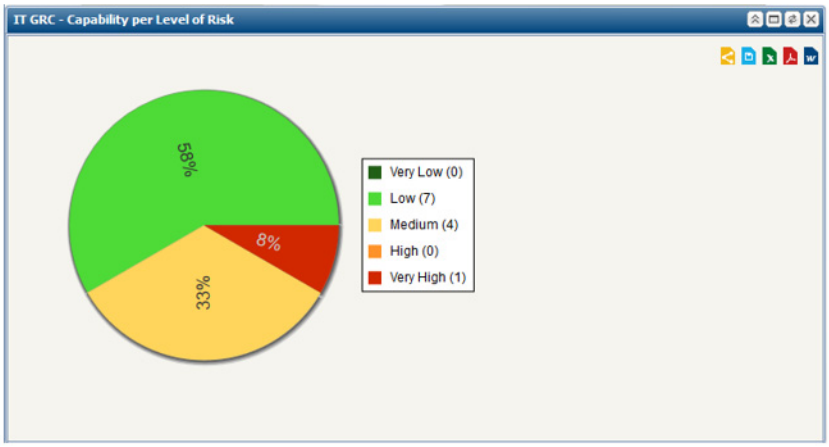


To display the corresponding processes, click on the area in question.

Capacity widget by risk level

This a pie chart that displays the percentage of the total number of first-level capacities per risk level.

> ☛ *A business capability is a component of information system processing. Processing can for example correspond to an activity or an enterprise business.*



Risk causality report

See "Risk causality report", page 40.

Reports Concerning Vulnerabilities

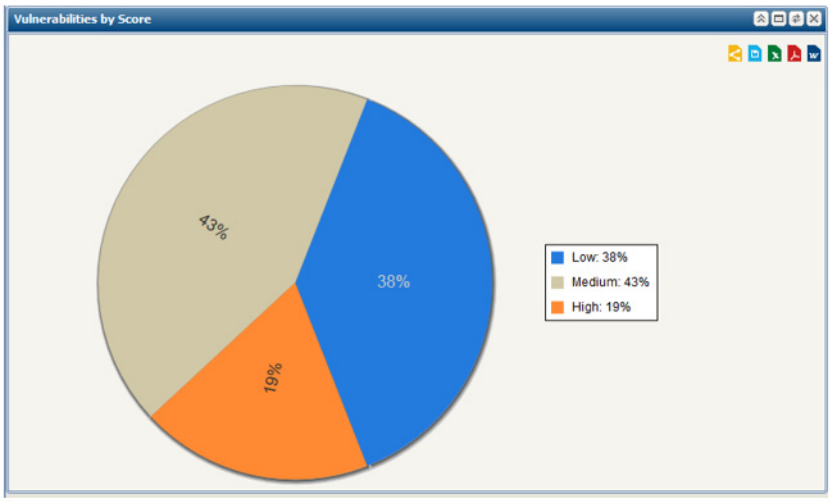
Widgets concerning vulnerabilities are provided as standard.

Vulnerability widget by score

This is a pie chart that displays the number of vulnerabilities per score:

- bottom
- medium
- high

> 🕮 *Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset.*



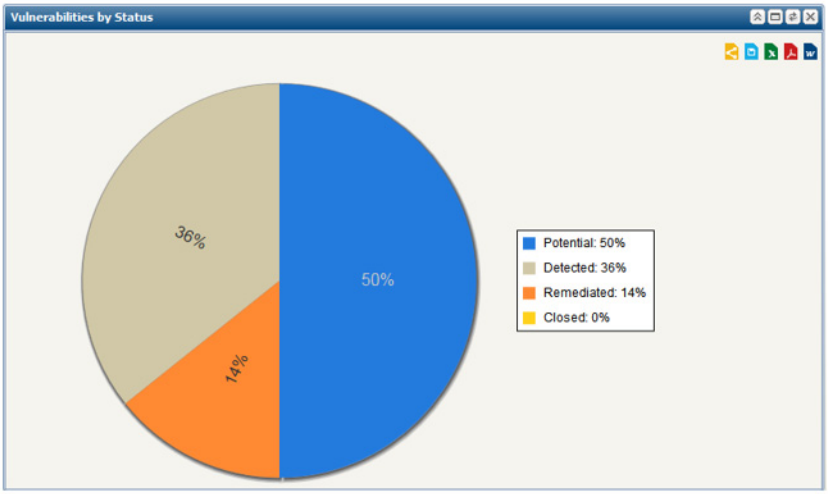
To display the corresponding vulnerabilities, click on the area in question.

Vulnerability widget per status

This is a pie chart that displays the number of vulnerabilities by status:

- potential
- detected
- remediated
- closed

> *Vulnerabilities are failures to control an IT asset that makes it vulnerable to a threat and can lead to a breach of confidentiality, lack of integrity or availability of this asset.*



To display the corresponding vulnerabilities, click on the area in question.

IT COMPLIANCE REPORTS

☛ *For more details, see "Managing IT Compliance", page 44.*

Control Identification

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

- by process

  ☛ *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.*

- by control type

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

- by entity

  🕮 *An entity can be internal or external to the enterprise: an internal entity represents an element in the organization of the enterprise such as a department, service or a workstation. 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.*

- by objective

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

- by regulatory framework

  🕮 *A regulation or regulatory 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.*

Access path

Reports > IT Compliance > Control Identification

Parameters

This consists of selecting the controls that will be presented in specifying elements that define their scope.

- control types
- entities
- processes
- objectives

Parameters	Parameter type	Constraints
Begin Date	date	Assessment selection criterion Not mandatory.
End date	date	Assessment selection criterion; set to current date.
Scope control type	control type	Control selection criterion. Not mandatory.
Scope entities	entity	Control selection criterion. Not mandatory.
Scope processes	process	Control selection criterion. Not mandatory.
Scope objectives	objectives	Control selection criterion. Not mandatory.

Result

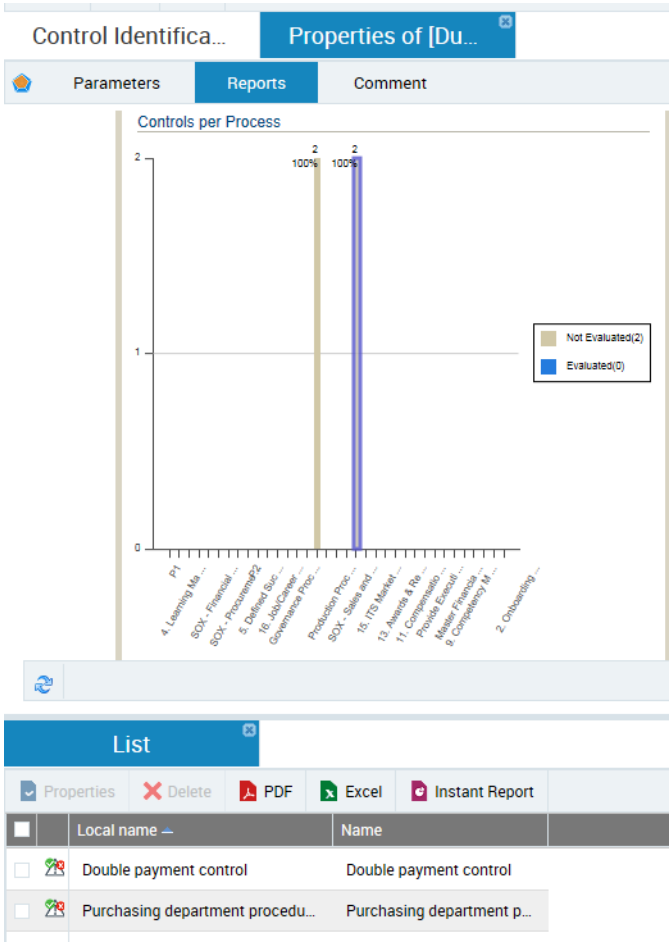
The report presents the distribution of controls in the form of a stacked bar chart. The distribution criteria are as follows:

- Distribution by process
- Distribution by control type
- Distribution by entity
- Distribution by objective
- Distribution by status
- Distribution by regulatory framework

Example

The bar chart below shows the number of controls (evaluated or not evaluated) by regulation.

When you click on a bar chart, the controls in question appear in a list at the bottom of the page.



Control Level by Regulation

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

Access path

Reports > IT Compliance > Control Level per Regulation Framework

Parameters

- End date: today's date by default
- Begin date: corresponds to the end date of the previous year
- Regulations: all regulations are used to filter the controls (mandatory)

  📖 *A regulation or regulatory 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.*

- Process (optional)

  📖 *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.*

Click **Generate Aggregation** to launch the calculations.

Result

This report is presented in tree form that displays an assessment for each element on the path. This path appears as seen here:

```
Regulation Framework > Requirements> Control Types >
Controls
```

Here is the meaning of each row:

Row	View
Controls	Control assessment average (%) for all connected applications.
Control types	Assessment average for all control types

☛ *A control belonging to different type is "counted" several times.*

Example

	Control Level	Design	Effectiveness
RF1	54%	100%	54%
Req 1	50%	100%	50%
CT1	50%	100%	50%
C1	50%	100%	50%
Req 2	58%	100%	58%
CT3	100%	100%	100%
C3	100%	100%	100%
CT1	50%	100%	50%
C1	50%	100%	50%
CT2	25%	100%	25%
C1	50%	100%	50%
C2	0%	100%	0%

Risk Level Aggregated by Business Process

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

Access path

Reports > IT Compliance > Control Level per Business Process

Parameters

- End date: today's date by default
- Begin date: corresponds to the end date of the previous year
- Process (mandatory)
- Regulations: used to filter controls to be taken into account (optional)

Click **Generate Aggregation** to launch the calculations.

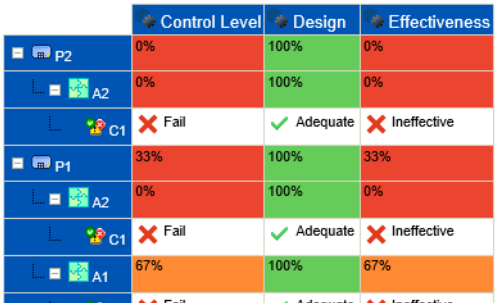
Result

This report is presented in tree form that displays the average of the most recent assessment for each element on the branch.

The tree is of the type: Business processes > Applications > Controls.

The row concerning the control provides the most recent control assessment in the context of the application.

Example



	Control Level	Design	Effectiveness
P2	0%	100%	0%
A2	0%	100%	0%
C1	Fail	Adequate	Ineffective
P1	33%	100%	33%
A2	0%	100%	0%
C1	Fail	Adequate	Ineffective
A1	67%	100%	67%

Compliance Widgets

Widgets are accessible from the dashboard via the home page.

They do not contain any parameters.

Process Compliance

This bar chart presents the control level for root processes.

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

To access the applications of the process:

1. Click on the corresponding bar.
   The list of process applications with their average compliance rate appears.

Regulatory compliance

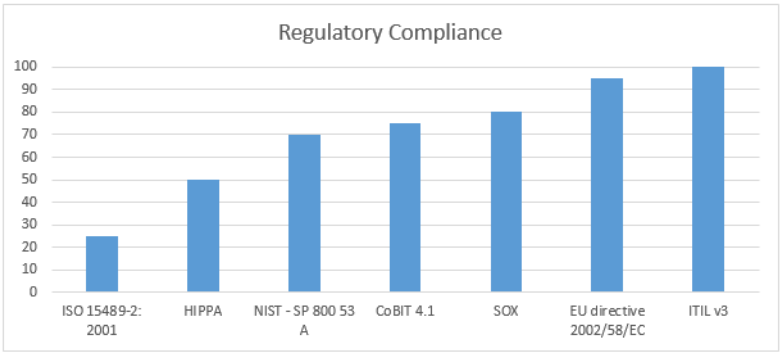
This is a bar chart presenting:

- y-axis: the root regulation frameworks

  📖 *A regulation or regulatory 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.*

- x-axis: the average control level

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



To access the requirements of the regulation framework:

❱ Click on the corresponding bar.

☛ *Any existing sub-regulation frameworks are not displayed.*

The list of requirements of the regulation framework with their compliance rate appears.

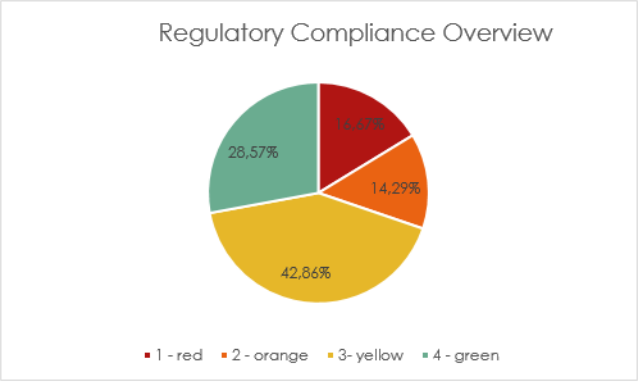
📖 *The compliance rate is the percentage of satisfactory controls per regulation framework.*

For more details on how to obtain compliance rates, see . "Assessing risks directly", page 42

Global control level

This pie chart presents the breakdown of regulation frameworks by compliance level.

> 🕮 *The compliance rate is the percentage of satisfactory controls per regulation framework.*
>
> 🕮 *A regulation or regulatory 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.*



To display the list of regulation frameworks associated with a sector in the chart:

- Click on the sector in question.

For more details on how to obtain compliance rates, see "Assessing risks directly", page 42.

VENDOR MANAGEMENT REPORTS

☛ *For more details on vendor management, see "Managing IT Vendors", page 47.*

Matrix Vendor by Vendor Type x Risk Level

Access path

Reports > IT Vendor Management > Matrix Vendor by Vendor Type x Risk Level

Parameters

N/A

Results

This report presents the number of vendors by risk level and vendor type. It is used to access the list of vendors.

To access vendors:

1. Click on the number that appears in the cells.
   The following information is provided for each vendor:
   - vendor type
   - vendor name
   - vendor risk assessment
   - Total amount of purchases (end of previous year)
   - Rank

   ☛ *For more details on entering this information, see "Characteristics of vendors", page 32.*

Example

⊟ 1. Matrix Vendor by Vendor Type X Risk Level

	Low	Medium	High
Services	0	0	0
Software	0	1	0
Software and Services	0	0	2
Total	0	0	0

Vendor Risk Level by Business Line

Access path

Reports > IT Vendor Management > Vendor Risk Level by Business Line

Parameters

N/A

Results

This report presents the number of vendors by risk level and business line.

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.

☛ *You cannot access the list of vendors from this report.*

Example

1. Risk Level By Business Line

	Low	Medium	High
Banking	0	0	0
Agency Services	0	0	0
Asset Management	0	0	0
Commercial Banking	0	0	0
Corporate Finance	0	0	0
Payment and Settlement	0	0	0
Retail Banking	0	0	0
Retail Brokerage	0	0	0
Trading and Sales	0	0	0
Industry	0	2	1
Sale by partner	0	2	1
Sale in Agency	0	2	1
Sale on Internet	0	2	1
Sale to the professionals	0	2	1
WholeSales	0	0	0
Total	0	2	1

ASSESSMENT REPORTS

☛ *For more details on assessments, see "Assessments by Questionnaires", page 49.*

Session Follow-Up

Access path

- Campaign Management > Follow-Up > Session Follow-up
- from an assessment session.

To access this report from an assessment session:

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

Parameters

- assessment session

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

Result

A summary displays general information on the current assessment session.

This report presents a number of charts concerning assessment progress:

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

Session Statistics

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

Access path

Campaign Management > Follow-Up > Session Statistics

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Result

A tree appears:

- in rows: questions/answers, together with respondents
- in columns: for each question/answer:
  - number of respondents
  - the objects concerned by the response

  This tree specifies who has answered what to which question.