Hopex GRC

Hopex Aquila

Bizzdesign

HOPEX GRC Common Features

User Guide

HOPEX Aquila 6.2

Bizzdesign

CONTENTS

About the GRC Manager Desktop

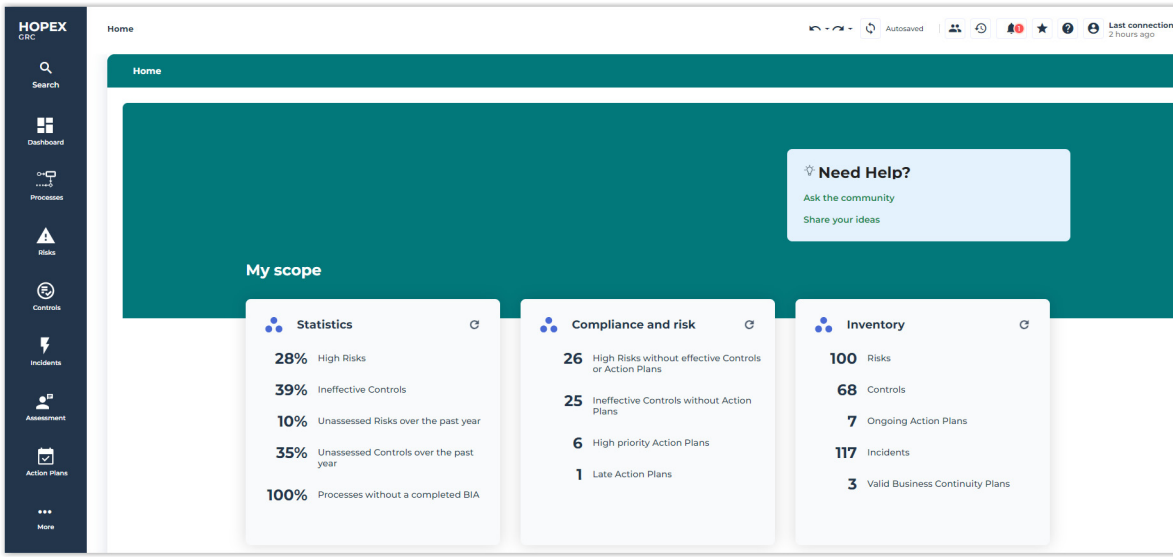
The Hopex GRC (Governance, Risk & Compliance) desktop is a central access point for risk, control, incident and audit users.

It is available with the following solutions:

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

  ☛ *For more details on **Hopex Internal Audit** see the corresponding documentation.*
- **Hopex BCM**

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



Different menus correspond to the main GRC-related object types as well as object types and features common to **Hopex**.

Search

See Full-text Search in the **Hopex Common Features** documentation.

Dashboard

This menu enables you to add widgets specific to risk, control management and audit.

Processes

See Managing Process Categories and Processes.

Risks

See Managing Risks.

Controls

See Managing Controls.

Incidents

See Collecting Incidents.

Assessment

See Assessment Campaigns.

See also the documentation specific to each solution:

- Assessing Risks
- Executing Controls.
- Assessing Controls

Action Plans

See Managing Issues and Action Plans.

Compliance

See Managing Compliance.

Testing

See Control Testing.

☛ *This menu is available with **Hopex Internal Control** only.*

Continuity

This menu deals with business continuity.

See Introduction to Hopex BCM.

☛ *This menu is available with **Hopex BCM** only.*

Reports

See GRC Reports.

Environment

See GRC Environment.

☛ *This menu is available to the GRC functional administrator only.*

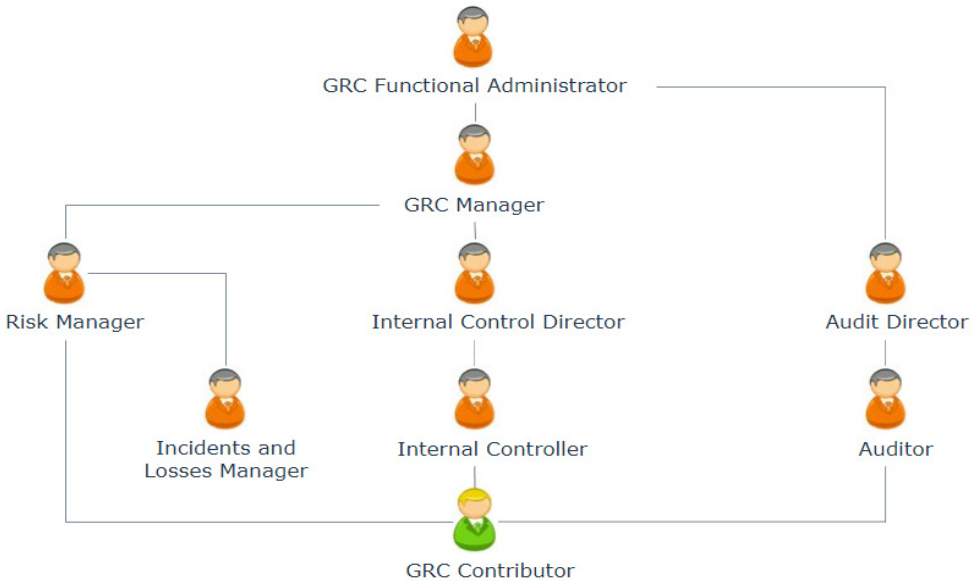
ACCESSING THE GRC DESKTOP

To connect to **Hopex**, see Logging in to Hopex.

In **Hopex GRC**,there are profiles associated to specific activities.

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

Profiles used in GRC solutions



Risk Manager

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

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

For more details, see Managing Risks.

Internal Control Director

The Internal Control Director:

- has all internal Controller rights

  ☛ *See Internal Controller.*

- validates campaigns
- prepares test plans
- validates action plans

For more details, see Managing Controls (Hopex Internal Control).

Incident and Loss Manager

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

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

He can deal with:

- declared incidents
- action plans and actions

For more details, see Collecting Incidents (Hopex LDC).

GRC manager

The "GRC Manager" profile is available if you have access to more than one solution among:

- **Hopex Internal Control** (IC),
- **Hopex Enterprise Risk Management** (ERM)
- **Hopex LDC**
- **Hopex BCM**

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

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

Internal Controller

The internal controller:

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

GRC functional administrator

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

☛ *The GRC functional administrator also has the same rights as the Audit Director.*

The GRC functional administrator:

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

GRC Contributor

The contributor performs his/her tasks in a simplified desktop. For more details, see Features Available to the GRC Contributor.

GRC Profiles/Solutions Summary

Solutions/ Profiles	***ERM***	***IC***	***LDC***	***BCM***
GRC functional administrator	X	X	X	X
GRC manager	X	X	X	X
GRC Contributor	X	X	X	X
Risk Manager	X			X
Internal Control Director		X		
Internal Controller		X		
Incident and Loss Manager			X	

THE GRC DOCUMENTATION

The GRC (Governance, Risk & Compliance) documentation is structured as follows:

Features shared by all GRC solutions

- GRC Environment
- Key Indicators
- Assessment Campaigns
- GRC Reports

  ☛ *For information on risks/controls/incidents, see:*

  - *Risk-Related Reports.*
  - *Reports Related to Controls*
  - *Reports Related to Incidents*
- GRC Solution Workflows
- Appendix - Computation Rules

Hopex Internal Control

- Managing Controls
- Assessing Controls
- Executing Controls
- Managing Compliance
- Control Testing
- Reports Related to Controls
- Managing Issues and Action Plans
- Reports Related to Controls

Hopex Enterprise Risk Management

- Managing Risks
- Assessing Risks
- Risk-Related Reports

Hopex LDC

- Collecting Incidents
- Reports Related to Incidents

Hopex BCM

- Managing BCM Systems
- Defining a Business Impact Analysis
- Designing a Business Continuity Plan
- Testing a Business Continuity Plan
- Managing Crises

GRC FUNCTIONAL ADMINISTRATION

So that the different participants can play their roles within the framework of a GRC (Governance, Risk & Compliance) project, the functional administrator must first create and manage the elements required to prepare the tasks for each of them.

☛ *You need to login with the "GRC functional administrator" profile for this.*

- ✓ Reusing Regulation Data
- ✓ Managing Teams
- ✓ Managing Currencies
- ✓ Configuring Time Sheets
- ✓ Managing Campaign Calendars
- ✓ Managing Steering Calendars
- ✓ Administrating Key Indicators

REUSING REGULATION DATA

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

> 🕮 *A regulation framework is a set of directives, compulsory or not, defined by a government in a law, by standard bodies as "best practices" or as an internal policy in an organization.*
>
> 🕮 *A requirement is a need or expectation explicitly expressed, imposed as a constraint to be met within the context of a project. This project can be a certification project or an organizational project or an information system project.*

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

> ☛ *For more details on regulatory frameworks, see Managing the Compliance Register.*

Converting Regulation Data

To convert regulation frameworks and requirements:

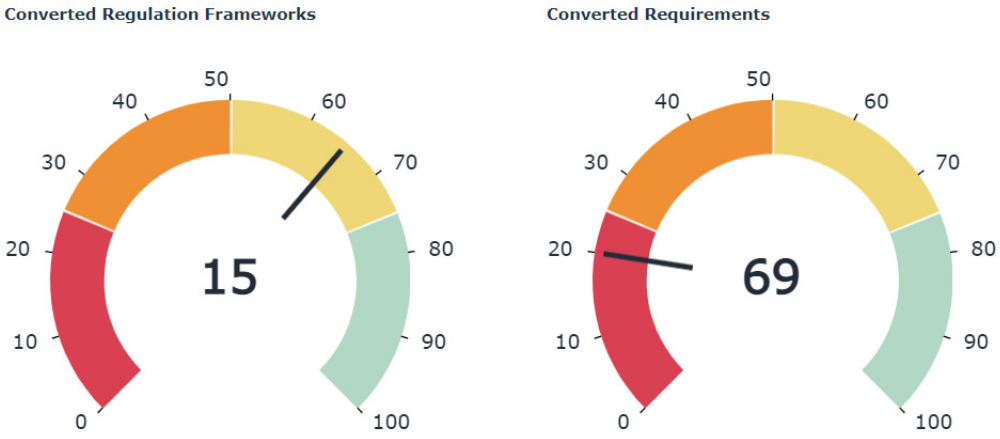
1. From the navigation bar, select **Administration > Tools > Regulation Data Conversion**.
   Gauges indicate the percentage of regulation frameworks and requirements which have been converted so far.
2. Click **Launch Data Conversion**.
3. In the **Convert into** column, indicate for each regulation framework if you want to:
   - convert it into a regulatory framework

     > 🕮 *A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), or standards.*
   - convert it into a business policy framework

     > 🕮 *A policy framework consists of a set of business policies. Policy frameworks may contain sections.*
   - do not want to convert it

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

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



Converted data can be viewed in the compliance register (**Compliance** menu. For more information, see Managing the Compliance Register.

☛ *The date of the regulation is not converted. Customized properties are not converted either.*

MANAGING TEAMS

You need to manage teams when using the following solutions:

- **Hopex Internal Control** (tests)
- **Hopex Internal Audit** (audits)

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

You must previously have defined:

- skill types
- skills list
- skill levels

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

Creating skill types

To create a skill type:

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

Creating skills

To create a skill:

1. In the navigation bar, select **Administration > Skill Management > Skills**.
2. Click **New**.
3. Enter a **Name** for the skill, for example "English".
4. Click **OK**.
   The new skill is added to the list of skills.
   In properties of the skill you can indicate the **Skill Type** to which it is attached, for example "Languages".

Creating skill levels

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

To create a skill level:

1. In the navigation bar, select **Administration > Skill Management > Skill Types**.
2. Open the properties of the skill type that interests you.
3. In the **Skill Levels** section, click **New**.
4. Enter a **Name**, for example "Beginner".
5. Click **OK**.

6. In **Skill Level Value**, enter a figure corresponding to the skill level, for example "1" for "Beginner" (while "4" could correspond with "Experienced" in our example).

   ☛ *This figure gives a graphic view of the extent of controller skills in the test assignment page.*

Viewing user skills

To view the skills of a user:

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

MANAGING CURRENCIES

Currencies are used:

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

Two currency types should be distinguished:

- central currency

  Central currency is the currency adopted as reference currency.

- local currency

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

Defining Central Currency

To define central currency:

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

Defining local currencies available to users

The GRC functional administrator must define local currencies available to users .

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

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

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

1. Login as a GRC Functional Administrator.
2. In the main menu, select **Settings > Options**.

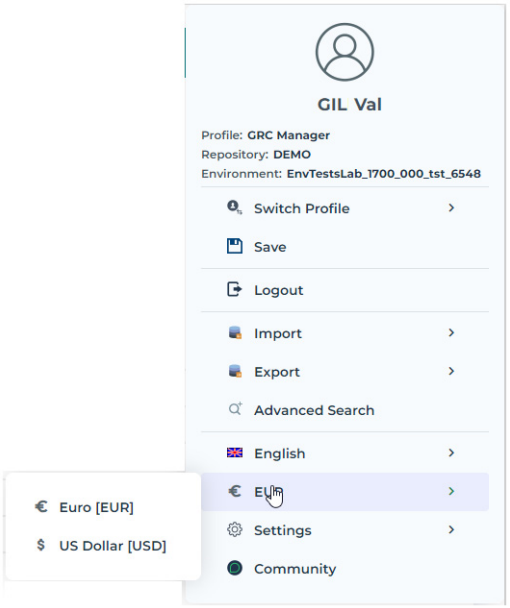
3. Select the **Installation > Currency** folder.
   The list of currencies available as standard appears on the right.
4. Select all the currencies that will be used locally by your users.
5. Click **OK**.

Specifying your local currency

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

To modify your local currency:

❱ In the main menu, select a currency as follows:



Managing Exchange Rates

To enter an exchange rate:

1. In the navigation bar, select **Administration > Tools > Exchange Rate**.
2. Click **New**.
3. In the window that appears, enter:
   - the **Currency Code To**.
   - the **Rate** of the source currency related to the final currency.
   - the **Rate Date Begin**.

☛ *Several exchange rate periods can be entered for the same currency. When entering expenses, the most recent exchange rate is taken into account.*

☛ *You must enter the exchange rate in both directions, for example:*

- *EUR->USD*
- *USD->EUR*

To view an exchange rate:

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

☛ *To reverse the exchange rate, click button* 

CONFIGURING TIME SHEETS

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

The GRC functional administrator can configure time sheet default options.

The GRC functional administrator can define:

- the number of hours worked per day
- non-working days in the company

To configure this data:

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

Managing Campaign Calendars

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

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

Creating schedules

To create a calendar:

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

You can then define calendar periods.

Creating calendar periods

To create calendar periods:

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

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

Connecting a calendar to an audit or test plan

To connect a calendar to an audit or test plan:

1. In the navigation bar, click:
   - **Audits > Audit Plans**
   - **Testing > Test Plans**
2. Open the properties of plan that interests you.
3. Click **Characteristics**.
4. In the **Calendar** field, select the calendar to connect.

MANAGING STEERING CALENDARS

Steering calendars are used within the framework of:

- execution campaigns

  ☛ *See Preparing Control Execution.*

- action plan reminders

To create and parameterize a steering calendar:

1. In the navigation bar, select **Administration > Calendars > Steering Calendars**.
2. Click **New**.
3. In the wizard that appears, select the context in which you want to use the steering calendar:
   - Control
   - Key Indicator
   - Action plan
   - Recommendation
4. Connect a **Steering Date** (which corresponds to the execution frequency of interest).
5. Open the steering date properties dialog box and select the **Scheduling** tab.
6. Specify the information required for starting the campaign including:
   - the time zone to take into account (UTC, user time zone, server time zone)
   - the start date of the recurrence

     ☛ *The start date specified on the steering calendar does not correspond to the campaign start date. It simply helps define the interval within which assessment sessions can take place.*

     ☛ *It is recommended to use a relative begin date on the steering date.*

   - start date and time

     ☛ *For details on possible configurations, see the section concerning the scheduler in the technical article "HOPEX Studio".*

     ☛ *Select **Execute at start date & time** if you wish to launch the campaign execution immediately.*

     If the check box is deactivated, the scheduler waits for the next recurrent date (and time) to trigger the job.

ADMINISTRATING KEY INDICATORS

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

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

Accessing Indicator Administration Features

To access GRC indicator administration features:

1. Login as a GRC Functional Administrator.
2. In the navigation bar, select **Administration > Indicators**.

You can view:

- indicator categories

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

- interpretation logics

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

- indicator statuses

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

- Aggregation periods

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

- Aggregation methods

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

Managing Indicator Categories

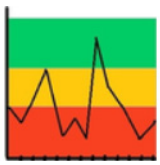
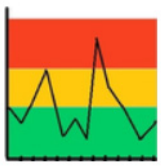
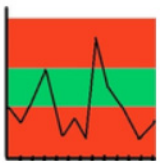
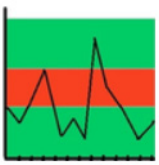
The key indicator category enables to specify how indicator values are interpreted, in order to compute the indicator status and Time to Failure.

To view indicator categories:

- In the navigation bar, select **Administration > Indicators > Categories**.

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

> 🕮 *Time to failure is the number of days before the key indicator turns to "Failed" status.*
>
> ☛ *The macro used to compute statuses is defined on key indicator interpretation logics. For more information, see Managing Indicator Interpretation logics.*

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

Managing Indicator Interpretation logics

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

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

To create key indicator interpretation logics:

1. In the navigation bar, select **Administration > Indicators > Interpretation logics**.
2. Click **New**.
3. In the window that opens, specify the **Indicator category** to which it is connected.
4. Specify the **Macro** used to compute indicator statuses.

   ☛ *The macro used to compute Time to Failure is defined on the Indicator category. For more information, see Managing Indicator Categories.*
5. In the **Indicator statuses** field, select the different statuses available for the indicators that use this interpretation logic.
6. Click **OK**.

Managing Indicator Statuses

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

Creating indicator statuses

To create indicator statuses:

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

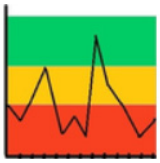
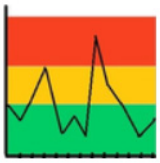
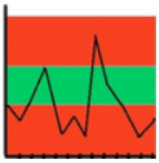
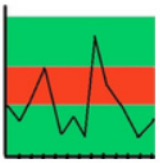
The new status you have just created will appear in the list of statuses available when creating an indicator interpretation logic. For more information, see Managing Indicator Interpretation logics.

Computation of indicator statuses

The following statuses are available by default:

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

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

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

Indicator status formulas

```
M = (Lower Threshold + Higher Threshold)/2
Low = Lower Threshold
High = Higher Threshold
```

Standard category

The Key Indicator status improves as its value increases.

Status	Formula
Unknown	No available values
Failed	KRI < Low
Operational	KI >= Low + 1.5*(High-M)
Warning	KI < Low + 1.5*(High-M) AND KI >= Low + 0.75*(High-M)
Unsatisfactory	KI < Low + 0.75*(High-M) AND KI >= Low + 0.25*(High-M)
Critical	KI < Low + 0.25*(High-M) AND KI >= Low

Accepted Values category

Status	Formula
Unknown	No available values
Failed	KI > High OR KI < Low
Operational	KI >= M - 0.5*(High-M) AND KI <= M + 0.5*(High-M)
Warning	KI > M + 0.5*(High-M) AND KI <= M + 0.75*(High-M) OR KI < M - 0.5*(High-M) AND KI >= M - 0.75*(High-M)
Unsatisfactory	KI > M + 0.75*(High-M) AND KI < M + 0.9*(High-M) OR KI < M - 0.75*(High-M) AND KI > M - 0.9*(High-M)
Critical	KI > M + 0.9*(High-M) AND KI <= High OR KI < M - 0.9*(High-M) AND KI >= Low

Rejected Values category

Status	Formula
Unknown	No available values
Failed	KI <= High AND KI >= Low
Operational	KI < Low - 0.5*(High-M) OR KI >= High + 0.5*(High-M)
Warning	KI < High + 0.5*(High-M) AND KI >= High + 0.25*(High-M) OR KI >= Low - 0.5*(High-M) AND KI < Low - 0.25*(High-M)
Unsatisfactory	KI < High + 0.25*(High-M) AND KI >= High + 0.1*(High-M) OR KI >= Low - 0.25*(High-M) AND KI < Low - 0.1*(High-M)
Critical	KI > High AND KI < High + 0.1*(High-M) OR KI < Low AND KI >= Low - 0.1*(High-M)

Reverse category

The Key Indicator status improves as its value decreases.

Status	Formula
Unknown	No available values
Failed	KI > High
Operational	KI <= High – 1.5*(High-M)
Warning	KI > High – 1.5*(High-M) AND KI <= High – 0.75*(High-M)
Unsatisfactory	KI > High – 0.75*(High-M) AND KI <= High – 0.25*(High-M)
Critical	KI > High – 0.25*(High-M) AND KI <= High

Managing Aggregation Periods and Methods

Aggregation periods

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

The following aggregation periods are available by default:

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

Aggregation methods

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

The following aggregation methods are available by default:

- Sum
- mean
- Max
- Min

Creating aggregation periods or methods

To create aggregation periods or methods:

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

Managing Key Indicator Value Computation Logics

You can define computation logics applicable to key indicator values.

Creating a computation logic

To create your own computation logic:

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

Key Indicator Value Computation Logics provided as default

Computation logic via query

The "computation logic via query" logic counts the number of objects returned by the query.

This logic accepts two parameters:

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

Percentage computation via query

The "percentage computation via query" logic counts the number of objects returned by queries and computes a percentage:

"NumeratorQuery" / "DenominatorQuery" * 100%

This computation logic accepts 3 parameters:

- "NumeratorQuery" (mandatory)
- "DenominatorQuery" (optional)
- "ObjectParameter" (optional)

Condition	Result or Action
If "DenominatorQuery" not specified	Denominator = total number of objects of the same type as the numerator
If "NumeratorQuery" requires an object as a parameter	Specify the parameter via "ObjectParameter"
If DenominatorQuery" requires an object as a parameter	Specify the same parameter as for "NumeratorQuery"

"RoundPrecision" defines the precision of the rounded value (number of digits after the decimal point).

If the denominator is 0, the computed value will be 0.

GRC ENVIRONMENT

This section explains how to view your environment in the **Hopex GRC** (Governance, Risk & Compliance) desktop.

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

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

ORGANIZATION

The enterprise organization is structured around the following concepts:

- Entities: see Managing Entities
- Processes: Managing Process Categories and Processes
- Business lines: Managing Business Lines
- Applications: Managing Applications
- Sites: Managing Sites

Managing Entities

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

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

Accessing organization entities

To access the different organization entities:

1. In the navigation bar, select **Processes > By entity**.
   The list of entities making up the organization is displayed.

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

Creating an entity

To create an entity:

1. See Accessing organization entities.
2. Click **New**.

Creating a sub- entity

To create a sub-entity:

1. See Creating an entity.
2. Drop it below the parent entity in the tree.

Defining entity general characteristics

In the entity property page, you can specify:

- its **Level** within the organization:
  - Business Unit
  - Sales
  - Service
- its **Status**:
  - Enabled
  - Disabled
- Its **Type**:
  - Vendor

    ☛ *The vendor is necessarily an "external" entity.*
  - Institution
  - Company
  - Public Department
  - Structure
  - Function
  - Generic
  - Responsible
- whether the entity is "Internal" or "External"

  ☛ *"Vendor" is an example of external entity.*
- its **Code**

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

Specifying responsibilities within an entity

You can specify responsible users within an entity.

You can specify different roles:

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

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

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

- **Risk Assessor**: person in charge of completing questionnaires about risks related to the entity.

  ☛ *You can define several risk assessors on the same entity.*

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

- **Control Assessor**: person in charge of completing questionnaires about controls related to the entity.

  ☛ *You can define several controls assessors on the same entity.*

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

- **Incident Approver**: person in charge of approving incidents that have an impact on the entity.
- **Incident Declarant:** The incident declarant is in charge of creating incidents within his/her scope.

  ☛ *For more information, see Incident Management Process.*

  ☛ *The incident declarant specified here will not need to specify an entity when creating an incident.*

- **Org-Unit Member**: this role enables to assign a user to an entity.

  Use case example: `display a user in the organigram, specify contacts for a vendor.`

To specify a responsibility, for example a Risk assessor:

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

Scoping an entity

An entity can be connected to different object types.

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

- **Risks**, whose management is assigned to the entity.

  ☛ *For more information, see Managing Risks.*

- **Controls**, whose management is assigned to the entity.

  ☛ *For more information, see Managing Controls.*

- **Incidents**
- **Action plans**

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

- **Entities**: you can specify the entity responsible for a service or management, as well as functional dependency between two entities.
- **Processes** for which the entity intervenes.

  ☛ *For more information, see Managing Process Categories and Processes.*
- **Objectives** assigned to the entity.

  ☛ *For more information, see Strategic Environment.*
- **Business Lines** for which the entity intervenes.

  ☛ *For more information, see Managing Business Lines.*

Managing Process Categories and Processes

Two process levels are available:

- process category

  A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.
- process

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

Accessing processes

To access the process category / process tree:

1. In the navigation bar, select **Processes**.

The processes and process categories appear.

Process hierarchy

The hierarchy of processes/operations is as follows:

Process category > Process > Operation

For each process of the hierarchy the following is displayed:

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

The following columns are available:

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

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

- **Forecast risk**

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

- **Latest compliance rate**

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

- **Control level**

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

Specifying process characteristics

To access process or process category properties:

1. Open the **Characteristics** page of its properties.

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

The **Responsible** user is in charge of planned actions (RACI).

Specifying process scope

A process / process category can be linked to different objects types.

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

- **Risks**: risks that relate to the process.

  For more information, see Managing Risks.

- **Controls**: controls that relate to the process.

  For more information, see Managing Controls.

- **Incidents**

  For more information, see Collecting Incidents.

- **Action plans**

  For more information, see Managing Action Plans.

  *To view regulations impacting a process, expand the **Regulatory Impact** section. For more information, see Managing the Regulatory Environment.*

Specifying responsibilities

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

To specify responsibilities on a process:

1. In the process properties, expand the **Responsibilities** section.
   You can specify the following responsibilities:
   - **Accountable**
   - **Consulted**
   - **Informed**

     ☛ *The above responsibilities correspond to the RACI responsibilities. See Responsibilities (RACI).*

     ☛ *The process **Accountable** is to be specified in the **Characteristics**.*
   - **Risk assessor**

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

     ☛ *You can define several risk assessors on the same entity.*
   - **Control assessor**

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

     ☛ *You can define several Control assessors on the same entity.*

Specifying sub-processes

To specify the sub-categories of a process category:

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

To specify the sub-processes of a process:

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

Managing business continuity

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

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

1. Open process or process category properties and select the **Business Continuity** page.

   ☛ *For more details, see:*

   - *Defining a Business Impact Analysis*
   - *Designing a Business Continuity Plan*

To add a process category to a BCM system:

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

   ☛ *For more information, see Managing BCM Systems.*

To create a Business Impact Analysis (BIA) from a process category:

- Right-click the process category and select **Create a BIA**.

Other sections of a process

The properties page of a process presents the following sections:

- **Objectives**: see Strategic Environment
- **IT assets**: It resources (applications, databases and servers) are made available for process implementation.

  ☛ *See Managing Applications.*
- **Entities** that intervene in the process.

  ☛ *See Managing Entities.*
- **Business Lines**: business lines that use the process services.

  ☛ *See Managing Business Lines.*

Managing Business Lines

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

Accessing Business Lines

To access the organization business lines:

- In the navigation bar, select **Environment > Organization > Business Lines**.

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

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

To access characteristics of a business line:

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

Connecting entities and processes to a business line

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

To connect a business line to entities and processes:

- In the business line properties, expand the following sections:
  - **Entities**

    ☛ *For more information, see Managing Entities.*
  - **Processes**

    ☛ *For more details, see Managing Process Categories and Processes.*

Defining risks and incidents that impact a business line

To specify risks that impact a business line:

- In the business line properties, select the pages:
  - **Risks**
  - **Incidents**

Entering gross revenues for incident management

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

☛ *For more information, see Gross Incomes.*

To specify gross revenues that impact a business line:

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

Managing Applications

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

Accessing applications

To access applications:

- In the **Hopex GRC** desktop, click **Environment > Organization > Applications**.

Specifying application scope

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

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

- Open the application properties and select:
  - **Characteristics > Processes**, or
  - **Characteristics > Business Lines**.

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

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

Managing business continuity

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

To access the Business Impact Analyses (BIAs) and Business Continuity Plans (BCPs) associated to an application:

1. Open the application properties and select the **Business Continuity** page.

☛ *For more details, see:*

- *Defining a Business Impact Analysis*
- *Designing a Business Continuity Plan*

Managing Sites

📖 *A site is a geographical location of an enterprise. Examples: Boston subsidiary, Seattle plant, and more generally the headquarters, subsidiaries, plants, warehouses, etc.*

Listing sites

To list sites:

1. In the **Hopex GRC** desktop, click **Environment > Organization > Sites**.

Managing business continuity

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

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

1. Open the site properties and select the **Business Continuity** page.

☛ *For more details, see:*

- *Defining a Business Impact Analysis*
- *Designing a Business Continuity Plan*

FINANCIAL ENVIRONMENT

To access components of the financial environment:

➢ In the navigation bar, click **Environment > Financial**.

Accounts

This tree displays controls associated to each account.

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

Characteristics of an account

Account characteristics are as follows:

- **Account type**
  The profits and losses account presents a description of profits and losses of the enterprise during the fiscal period. You can specify if the account is:
  - "Profits"
  - "Losses"
- **Total Value**: you can enter a total for this account.

  ☛ *An order of magnitude is sufficient.*
- **Status**
  - "Open": the account is active
  - "Closed": the account is inactive
- **Sub-accounts**: the account may consist of sub-accounts.
- **Entities** and **Processes**: you may connect the account to entities and processes.
- **Incident Financial Elements**:
  - Loss
  - Gain
  - Recovery
  - Provision

Connecting controls to an account

To connect controls to an account:

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

Products

This tree displays open issues related to the product.

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

To create or connect incidents to a product:

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

You can view, for each incident:

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

Gross Incomes

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

> ☛ *For more information, see Basic Indicator Approach (BIA).*

To create a gross income:

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

STRATEGIC ENVIRONMENT

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

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

To access the tree of objectives within your organization:

- In the navigation bar, select **Environment > Organization > Objectives**.

To create an objective:

- Click the **New** button.

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

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

RISK ENVIRONMENT

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

Describing Risk Environment

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

1. In the **Hopex GRC** desktop, click **Environment > Environment > Risks**.

   ☛ *The risk types are defined in **Risks > By Risk Type**.*

You can define:

- Risk factors

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

- Risk consequences

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

Defining the Environment of a Specific Risk

To define the environment for a specific risk:

1. In the **Characteristics** page of the property window of a risk, expand the **Analysis** section.
   A risk is characterized by:
   - **Risk types**

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

   - **Risk factors**

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

   - **Risk consequences**

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

   - **Associated Risks**

Risk types

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

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

Creating a risk type

To create your own risk types:

1. In the navigation bar, click **Risks > By Risk Type**.
2. Click **New**.
3. Enter the name of the risk type and click **OK**.
   The new risk type appears in the navigator menu tree.

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

Analyzing the impacts of a risk type

A report enables you to analyze the impacts of a risk type. See Risk Type Impact Breakdown.

Risk Factors

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

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

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

Risk consequences

To define consequences associated with a risk:

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

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

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

CONTROL ENVIRONMENT

To describe control environment and access sub-control types:

- In the navigation bar, click **Controls > 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.).

To view sub-control types and controls:

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

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

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

THE COMPLIANCE ENVIRONMENT

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

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

- In the navigation bar, select **Compliance > Regulations**.

You may:

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

  A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), or standards.

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

  Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.
- create manually policy frameworks and business policies.

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

Managing your Regulatory Environment

Using UCF Import

UCF Import Prerequisites

Internal Control directors and GRC Managers can upload UCF content (authority documents, citations and controls) and update it.

To be able to import this content to **HOPEX UCF**, you must have:

- **Hopex GRC** (or **Hopex Internal Control** as a minimum) AND **HOPEX UCF**
- a UCF account and API key
- a Shared List with the Authority Documents you want to import.

  ☛ *For more information, see Unified Compliance Framework.*
- parameterized UCF options in **HOPEX UCF**

  ☛ *In the UCF Common Controls Framework, information is generally available in English.*

  *If you want to use **HOPEX UCF** with **Hopex** user data language other than English, you must:*

  - *set up your data language of interest (example: if you want to use **Hopex** with French as data language, make sure to set up French as data).*
  - *import UCF data*
  - *repeat the operation (change data language + proceed to import) as many times as desired languages.*

Parameterizing UCF Import

To parameterize UCF import:

1. In the **Main menu**, select **Settings > Options**.
2. In the Options window, expand **Data Exchange > Import > UCF Common Controls Hub Integration**.
3. Select the **Activate UCF Import** check box.
4. Enter the URL corresponding to UCF API.

   `https://api.unifiedcompliance.com/`
5. Enter your **UCF API Authentication Key**.

   ☛ *To retrieve your API authentication key in your Unified Compliance Framework workspace:*

   - *go to Settings > API Manager > API Keys.*
   - *Create Credentials and copy paste your API Key.*
6. Click **OK**.

Importing Data from the Common Controls Hub

Compliance officers need to set up the UCF environment in **HOPEX UCF**. This consists in:

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

To import UCF data:

1. In the navigation bar, select **Environment > Compliance > Regulatory Frameworks**.
2. Click **Import UCF content**.
3. Click **Next**.
4. Select the Shared List from your Common Controls Hub.
5. Click **Next**.

6. Select the Authority Document(s) you wish to import into **Hopex**.

> ☛ *If you update an already imported Authority Document, it may be useful to compare the columns **Latest available UCF updates** and **Last imported UCF update**.*

7. Click **Next**.

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

Creating Regulatory Content Manually

Creating regulatory frameworks and their content

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

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

To create a regulatory framework:

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

> 🕮 *A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), or standards.*

To create content for your regulatory framework:

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

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

   - **New > Regulation Article**

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

Creating control directives

To create control directives:

1. In the navigation bar, click **Compliance > Relevant Regulations > Control Directives**.
2. Right-click the root of the tree and select **New > Control Directive**.

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

Managing Business Policies

Hopex GRC enables you to manage both business policies and regulations.

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

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

To create a policy framework:

1. In the navigation bar, **Compliance > Regulations > Policy Frameworks**.
2. Click **New**.

To create policy framework content:

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

Defining Applicable Regulations and Business Policies

Regulatory content applicability

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

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

Compliance officers can inspect the imported regulatory frameworks and specify which ones are applicable. Only applicable content can be viewed by stakeholders in **Hopex** registers. See Managing the Compliance Register.

Reviewing regulatory frameworks after UCF import

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

This tree displays:

- regulatory frameworks (Authority Documents)
- citations (Citations)
- associated control directives (Common Controls)

It is based on the supported/supporting structure originally defined by UCF.

From this tree you can:

- review the newly imported regulatory frameworks and their content.
- Indicate which pieces of regulatory content are deemed relevant to your organization.

Selecting the regulatory content applicable to your organization

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

To declare regulatory content as applicable:

1. In the navigation bar, select **Compliance > Regulatory Frameworks**.

2. Expand the tree if necessary and select the check-box corresponding to the regulatory frameworks/articles/sections you must comply with.

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

Defining the Scope of Regulations and Business Policies

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

To do this:

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

RESPONSIBILITIES (RACI)

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

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

Responsibility levels

The proposed responsibility levels are as follows:

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

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

- on a process category or a process,
- on a risk
- on a control

Specifying Responsibilities

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

To specify the persons concerned by a specific object:

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

KEY INDICATORS

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

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

To administrate key indicators, see Administrating Key Indicators.

☛ *Key indicators are available with **Hopex Internal Control** and **Hopex Enterprise Risk Management**.*

ACCESSING KEY INDICATORS

To access the key indicators from a list:

1. In the navigation bar, select **Environment > Indicators**.
   A list of all the indicators of your environment is displayed.

The following information is displayed in columns for each indicator:

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

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

- Value
- Lower Threshold
- Higher Threshold
- Entities

  ☛ *For more information on the information provided in columns, see Defining Key Indicators.*

DEFINING KEY INDICATORS

Creating a Key Indicator

To create a key indicator:

1. In the navigation bar, select **Environment > Indicators**.
2. Click **New**.
   A creation window opens.

   ☛ *You may also create a key indicator from the home page (**Quick access > Actions > Create a Key Indicator**.*
3. Specify a **Lower Threshold** and a **Higher Threshold**.
4. Specify an indicator **Category**.
   The indicator category determines how the indicator values are interpreted and how the indicator status is computed:
   - the higher threshold represents the objective.
   - **Reverse**: opposite of standard
   - **Accepted Values**: All the values within the thresholds are accepted.
   - **Rejected Values**: all values within the defined thresholds are rejected.

   ☛ *If several algorithms are provided for an indicator category, the field **Key Indicator Interpretation logics** is proposed. You can select the desired algorithm to compute the indicator status. For further details, see Relation between Indicator Category and Interpretation Logic.*
5. Specify whether you need to aggregate values over a specific period of time.
   The aggregation is not specified by default.

   ☛ *If you need to aggregate values, see Specifying the Aggregation Period and Method.*
6. Click **OK** to create your indicator.

   ☛ *You cannot change the key indicator category, aggregation period and aggregation method after the key indicator has been created.*

Specifying the Aggregation Period and Method

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

To aggregate values:

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

2. Specify the **Aggregation period**.

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

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

3. Specify the **Aggregation Method**.

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

   - Sum
   - Average

   ☛ *Note that new aggregation periods and aggregation methods can be created by your functional administrator.*

   ☛ *Once the key indicator has been created, it is no longer possible to specify another aggregation period or method.*

Example of a Key Indicator

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

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

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

The key indicator monitors the monthly turnover. This is to ensure that the appropriate measures are taken if things do not go as expected.

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

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

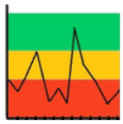
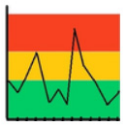
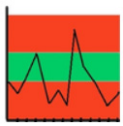
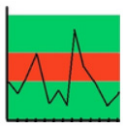
- **Lower Threshold** 900k
- **Higher Threshold** 1100k
- **Category**: Standard (all values beyond the upper limit are considered satisfactory)
- **Aggregation period**: monthly
- **Aggregation method**: sum
- **Statuses** for the monthly turnover:

Operational	>= 1050
Warning .	>= 975 and < 1050
Unsatisfactory	>= 925 and < 975
Critical	>= 900 and < 925
Failed	< 900

KEY INDICATOR CATEGORIES

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

Description of Key Indicator Categories

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

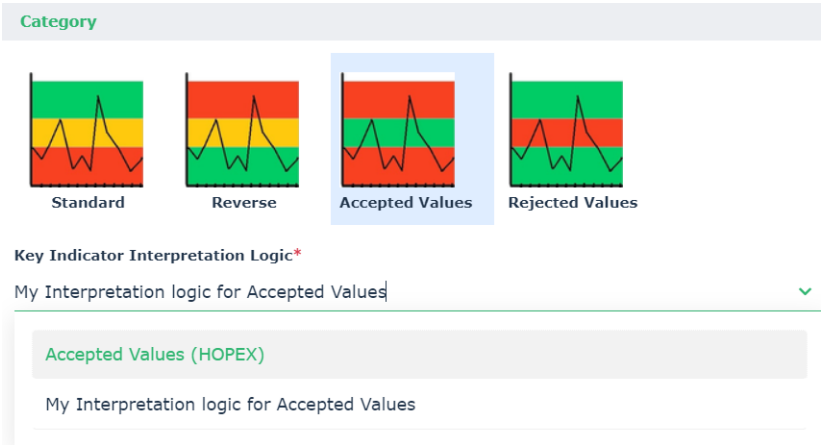
Relation between Indicator Category and Interpretation Logic

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

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

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

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



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

DETAILING KEY INDICATORS

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

> ☛ *You cannot change the key indicator category, aggregation period and aggregation method after the key indicator has been created.*

Editing Key Indicator Parameters

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

To edit parameters:

1. See Accessing Key Indicators.
2. In the **Characteristics** indicator property page, expand the **Advanced** section.
3. Click **Edit Parameters**.
   In the window that opens, you can edit:
   - the **Lower Threshold** and the **Higher Threshold**.
   - the **Number of values used to compute Time to Failure**.

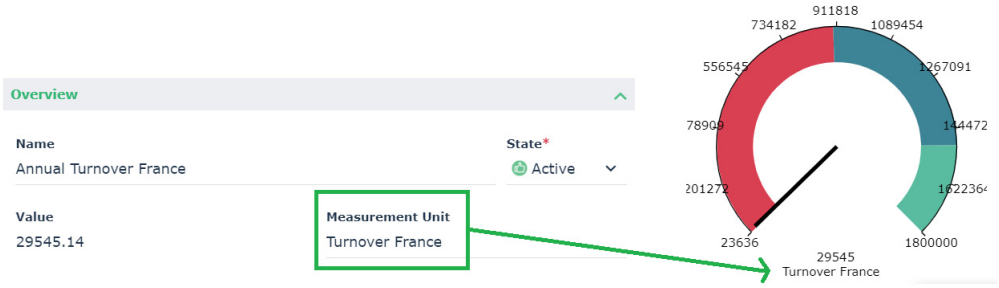
> 🕮 *Time to failure is the number of days before the key indicator turns to "Failed" status.*

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

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

Defining a Measurement Unit to be Displayed in Reports

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



For more details on graphs and reports, see Viewing the Indicator Graph.

Activating / Deactivating a Key Indicator

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

To deactivate a key indicator:

1. See Accessing Key Indicators.
2. Open the key indicator property page.
3. In the **State** field, select "Inactive".

If you set the state to "Inactive":

- The value and status of the key indicator is computed one last time
- It is no longer possible to enter new values
- All current notifications are deactivated

> ☛ *To be able to enter new values again and/or edit the properties of the key indicator, set the State to "Active".*
>
> ☛ *The state of a key indicator should be distinguished from its status.*

Specifying the Indicator Scope

To specify the scope of the indicator:

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

Here you can specify the associated objects:

- entities

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

- process categories

  📖 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

- process

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

- Applications

To remove indicators to a given entity:

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

Specifying Action Plans

To define action plans on a key indicator:

1. See Accessing Key Indicators.
2. In the properties of a key indicator, select the **Action Plans** page.
3. Connect an existing action plan or create one as appropriate.

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

   ☛ *For more information on action plans, see the corresponding information in the Common Features section of this Online help.*

Connecting Risks

To connect risks to a key indicator:

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

KEY INDICATOR OVERVIEW

☛ *See Accessing Key Indicators.*

The **Overview** property page gives access to:

- A card of the key indicator, which gives an overview of its main characteristics.

  ☛ *For more details, see Card of an Object in the "Platform - Common Features" section.*

- Computed information in the form of a dashboard

Indicator Status

Default statuses

The following statuses are available by default:

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

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

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

The indicator status enables to issue a warning when necessary. For further details, see Defining Measurement Frequency and Notifications.

Information about indicator status computation

The indicator status is computed based on:

- the indicator latest values

  ☛ *For more details on indicator values, see Entering Periodic Key Indicator Values.*

- the aggregation period

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

- the aggregation method

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

  ☛ *For further details, see Specifying the Aggregation Period and Method.*

The key indicator status is computed when:

- a new value is added

  ☛ *For further details, see Entering Periodic Key Indicator Values.*

- an existing value is deleted
- key indicator thresholds are edited
- the indicator state (active or inactive) has been modified

  ☛ *For further details, see Activating / Deactivating a Key Indicator.*

Time to Failure

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

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

You must specify the number of past values taken into account to compute Time to Failure. For further details, see Key Indicator Overview.

Value	Details
Unknown	Not enough data available (at least 2 aggregated values should be available)
Unforeseen	The indicator values evolve in a way which makes it impossible to reach/predict the Failed status. ☛ *9999 is displayed in the Time to Failure column of the list of indicators.*
0 day(s)	The indicator status is "Failed" already.

Last Measurement of the Key Indicator

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

This value is rounded to the closest integer.

Key Indicator Value

In the key indicator identification card, you can also find the Value of the key indicator.

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

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

See also: Entering Periodic Key Indicator Values.

DEFINING MEASUREMENT FREQUENCY AND NOTIFICATIONS

Specifying Measurement Frequency

To specify the measurement frequency of an indicator:

1. See Accessing Key Indicators.
2. In the properties of a key indicator, select the **Values** page.
3. In the **Measurement Settings** section, select a steering calendar (**Measurement Frequency** field):
   - **Daily** Measurement Frequency
   - **Monthly** Measurement Frequency
   - **Weekly** Measurement Frequency

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

Managing Notifications

Hopex GRC enables to send automatic notifications based on:

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

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

To specify or modify user notifications:

1. See Accessing Key Indicators.
2. In the properties of a key indicator, select the **Notifications** page.

You can choose to send periodic notifications:

- to a specific person

  ☛ *By default, the owner of a key indicator receives notifications. Here you can specify another person.*

  ☛ *The notifications sent to appropriate users prompts them to enter values for the key indicator they are in charge of monitoring. For further details, see Entering Periodic Key Indicator Values.*

- to a set of users (when the indicator reaches a specified status or when the last measurement is older than a specified number of days).

Entering Periodic Key Indicator Values

Hopex GRC enables the indicator owner or other authorized persons to manually enter key indicator values in order to feed the key indicator.

It is also possible to feed automatically the key indicator.

Entering a key indicator value manually

To enter a key indicator value:

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

> ☛ *Notifications can be set up so that you are periodically reminded of the need of entering periodic values. For further details, see Managing Notifications.*

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

Parameterizing automatic value entering

It is also possible to feed automatically the key indicator.

To do this:

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

> ☛ *For further details, see Managing Key Indicator Value Computation Logics.*

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

```
Query =
ObjectParameter =
```

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

VIEWING THE INDICATOR GRAPH

Hopex GRC enables you to display an indicator graph for a specific indicator.

To access this graph:

1. See Accessing Key Indicators.
2. In the property page of your indicator, select the **Indicator Graph** page.

> ☛ *This graph is also available in the **Overview** page of the indicator properties.*

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

> ☛ *To display a label on the Y axis of the graph, see Defining a Measurement Unit to be Displayed in Reports.*

Hopex GRC also offers reports which enable to compare various indicators. See Key Indicator Reports.

ASSESSMENT CAMPAIGNS

GRC solutions (Governance, Risk & Compliance) allow you to assess controls and risks through assessment campaigns.

- ✓ Accessing Assessments by Profiles
- ✓ Accessing Assessment Templates
- ✓ Preparing the Assessment Environment
- ✓ Starting an Assessment Campaign

See also:

- Following up Assessment Progress
- Managing Questionnaires

ACCESSING ASSESSMENTS BY PROFILES

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

Profile	Action	Desktop
GRC functional administrator	- Assign roles to persons of the enterprise - Define the organization (entities, processes,...) - Determine respondents (risk assessors for each entity)	Hopex GRC desktop
GRC manager (Internal Controller)	- Create assessment campaigns - Create assessment sessions - Follow up assessment sessions	Hopex GRC desktop
GRC Contributor	- Accept or refuse questionnaires Reply to questionnaires	GRC Contributor desktop

ACCESSING ASSESSMENT TEMPLATES

☛ *To view assessment templates you need to login as a GRC functional administrator.*

To access assessment templates:

1. In the navigation bar, click **Administration > Assessment > Assessment Templates**.
   Assessment templates appear.

The assessment templates use:

- assessed characteristics

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

- a questionnaire template

  🕮 *A questionnaire template represents definition of questionnaire content.*

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

  For more details on assessment template customization, see Managing Assessment Templates.

PREPARING THE ASSESSMENT ENVIRONMENT

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

Prerequisites to Risk Assessment

For risk assessment, see Prerequisites to Risk Assessment.

Pre-requisites to Control Assessment

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

- Control Assessment by Entity
- Control Assessment by Entity and Regulatory Framework

STARTING AN ASSESSMENT CAMPAIGN

Creating Assessment Campaigns

To create an assessment campaign in **Hopex GRC**:

1. In the navigation bar, click **Assessment > Campaigns**.
2. Click **New**.

   ☛ *You may also create an assessment campaign from the home page (**Quick access > Actions > Create an assessment campaign)**.*
3. Select the Questionnaire Template to be used:
   - **Risk Assessment by Entity and Process**
   - **Assessment of risks by application**

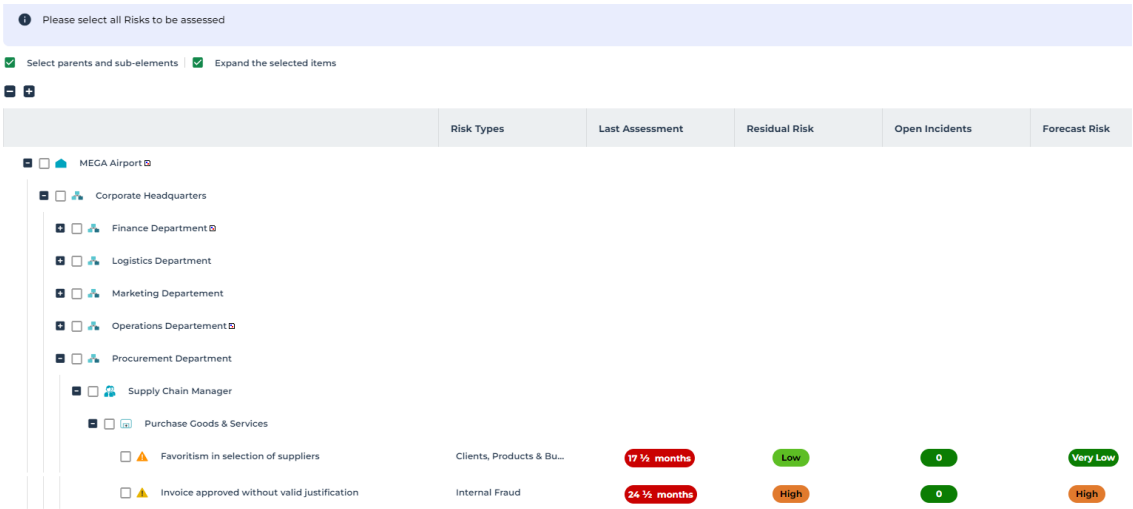
     ☛ *For more details, see Risk Assessment Templates.*
   - **Control assessment**
   - **Control Assessment by Entity and Regulatory Framework**

     ☛ *For more details, see Controls Assessment Templates.*
4. Click **Next**.
   The campaign creation page appears.
5. Specify the campaign **Name**.
6. Modify the **Calendar** if required.

   ☛ *The calendar serves to initialize the begin and end dates of the evaluation campaign.*
7. Specify the **Begin Date** and the **End Date**.
8. Click **Next**.

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

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



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

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

10. Click **Next**.

11. Look at the campaign summary.
    Elements that will be assessed appear.

Assessment summary (12)

Name	Respondent	Context	Last Assessment	Residual Risk	Open Incidents	Forecast Risk
Favoritism in selection of suppliers	Nicole	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services ➤ Make a Purchase Request	17 ½ months	Low	0	Very Low
Favoritism in selection of suppliers	Nicole	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services	17 ½ months	Low	0	Very Low
Favoritism in selection of suppliers	Nicole	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services ➤ Organize a call for tenders	17 ½ months	Low	0	Very Low
Invoice approved without valid justification	Simon	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services	24 ½ months	High	0	High
Invoice paid twice	Nicole	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services	24 ½ months	Medium	0	Very High
Invoice paid twice	Nicole	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services ➤ Place an Order (Purchase Request)	24 ½ months	Medium	0	Very High
Ongoing purchase budget not under control	Andrew	MEGA Airport ➤ Corporate Headquarters ➤ Procurement Department ➤ Supply Chain Manager ➤ Purchase Goods & Services	24 ½ months	Medium	0	Medium

In particular, you can view:

- ***assessed characteristics*** (defined in the assessment template)
- assessed ***objects*** (risks or controls)
- ***context objects*** (entities, processes, etc.)
- ***assessment nodes***, which correspond to objects placed in their context objects, associated with respondents.
- ***respondents***
- possible ***errors*** (it is not possible to launch the campaign without specifying some specific information, for example respondents)
- ***Warnings***, for information purpose (for example: missing e-mails)

12. Click **Next**.
13. In the page dedicated to planning, specify when you want the campaign to be started:
    - **Immediately**

      ☛ *If you choose this option, the campaign is started as soon as you click **OK**.*

    - **Specific Time and Date**

      ☛ *Your questionnaires will be sent to respondents at a specified date and time. This is the recommended option.*

    - **Not now**

      ☛ *No questionnaires are sent. You will need to manually create an assessment session when you are ready to plan the sending of questionnaires. See Creating an Assessment Session Manually.*

      ☛ *This option is not available if you have chosen to create the assessment campaign without a template.*

14. Click **OK**.

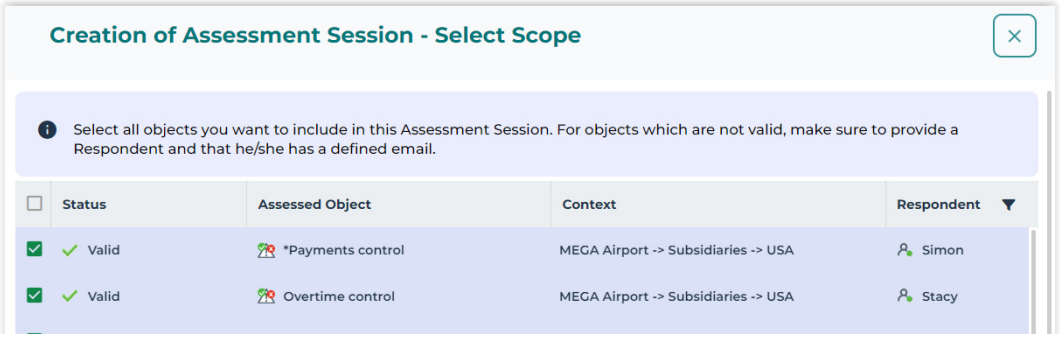
Creating an Assessment Session Manually

You must manually create one or several assessment sessions if you have selected the "Not now" scheduling option when creating the assessment campaign.

☛ *See Previous step: Creating Assessment Campaigns.*

To create an assessment session:

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



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

4. Click **Next**.
5. In the planning page, select whether you want to send questionnaires:
   - **Immediately**

     ☛ *If you select "Immediately", an assessment session is started right now.*

   - at a **Specific Time and Date**

GRC REPORTS

Several reports deal with global GRC-related issues (Governance, Risk & Compliance).

- Key Indicator Reports
- Action Plan Follow-up Reports

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

- Risk-Related Reports
- Reports Related to Controls
- IT Regulatory Compliance Reports
- Reports Related to Incidents

A summary table gives indication on report availability. See GRC Report Availability.

☛ *For more information on reports, see:*

- *Accessing Reports*
- *Creating a Report*
- *Managing Report Properties*

GRC Report Availability

Available reports depend on the profile and the solution used.

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

See also:

- Action Plan Follow-up Reports
- IT Regulatory Compliance Reports

KEY INDICATOR REPORTS

☛ *For more information on key indicators, see Key Indicators.*

Hopex GRC offers several reports to compare indicators.

The following reports are available:

- Indicator comparator
- Multi-Indicator Gauges
- Multi-Indicator Graph

☛ ***Hopex GRC** enables you to display a graph specific to an indicator. For more details, see Viewing the Indicator Graph.*

Indicator comparator

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

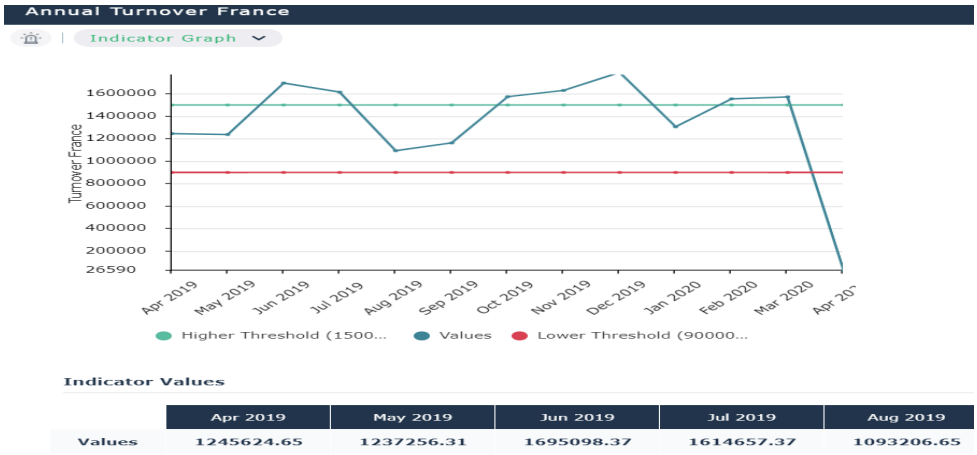
Access path

Navigation bar > Reports

Parameters

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

Results



Indicator Values

	Apr 2019	May 2019	Jun 2019	Jul 2019	Aug 2019
Values	1245624.65	1237256.31	1695098.37	1614657.37	1093206.65

Multi-Indicator Gauges

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

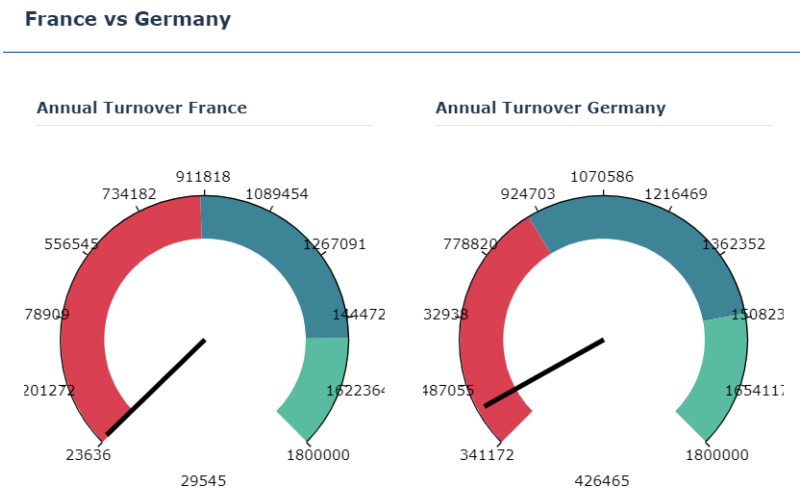
Access path

Navigation bar > Reports

Parameters

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

Results



Multi-Indicator Graph

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

Access path

Navigation bar > Reports

Parameters

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

Results

France vs. Germany

Annual Turnover France

Annual Turnover Germany

ACTION PLAN FOLLOW-UP REPORTS

For more information on action plans, see Managing Action Plans.

To access these reports:

- In the navigation menu, select **Reports**.

Action Plan Follow-Up (Dashboard)

Parameters

Parameters	Constraint
Action Plans or Libraries	Mandatory

Result

Action plans priority

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

Possible priorities are the following:

- Critical
- High
- Average
- Low

Action plan by organizational level

- global
- local

Action plans by status

- To be submitted
- To be validated
- To be sent
- Ongoing
- Completed
- Rejected

Action plans by origin

- Audit
- Compliance
- Event
- Other
- RFC
- Risk

Action plans by category

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

Examples of possible action plan categories:

- Audit recommendation
- Impact-reducing
- Control relevance improvement
- ...

Action Plans Accomplishment

- Succeeded
- Failed
- Not assessed

Top 10 Action Plans

Top 10 of action plans with higher priorities

Action Plan Follow-up Report (Dashboard)

Parameters

Parameters	Constraint
Begin Date	
End date	
Entities	Optional
Processes	Optional

Result

The number of action plans is displayed.

Several charts present the breakdown of action plans according to different criteria.

Action plans by status

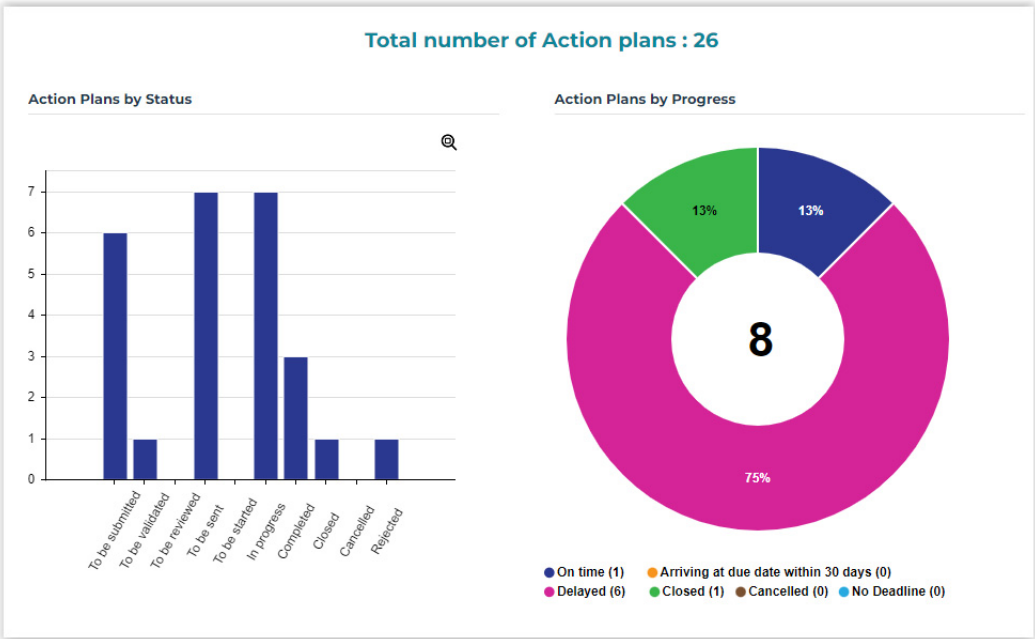
This bar chart presents action plan statuses:

- To be submitted
- To be validated
- To review
- To be sent
- To be started
- Ongoing
- Completed
- Closed
- Canceled

Action plans by progress

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

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



Action plan by priority

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

Possible priorities are the following:

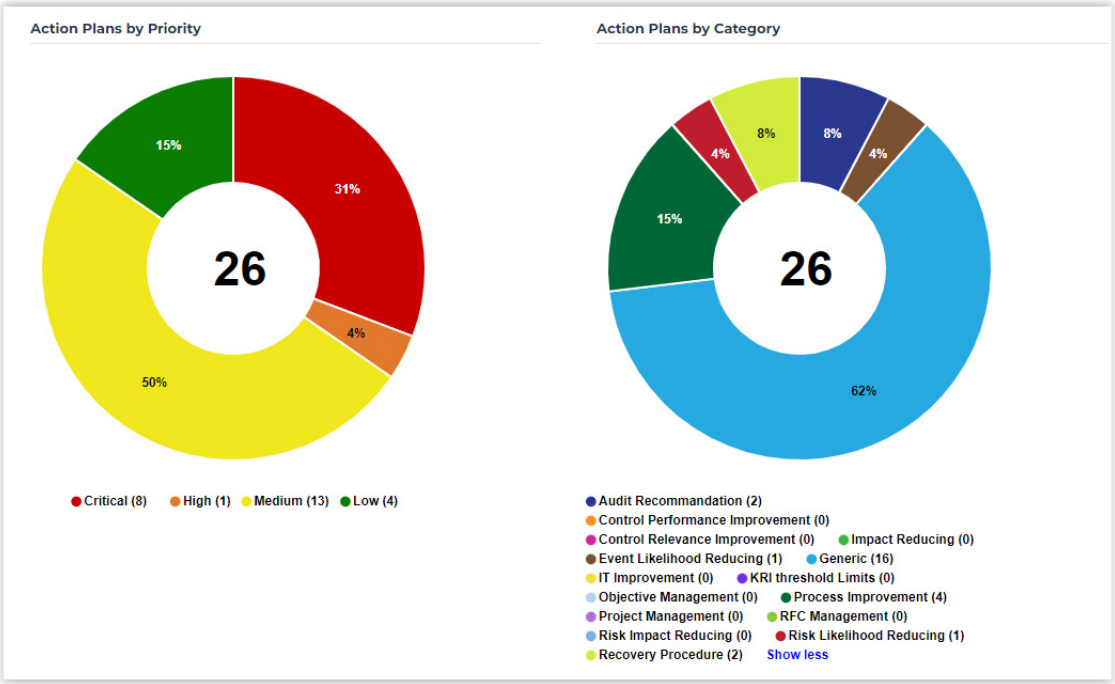
- Critical
- High
- Average
- Low

Action plans by category

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

Examples of possible action plan categories:

- Audit recommendation
- Impact-reducing
- Control relevance improvement
- ...



Action Plans by nature

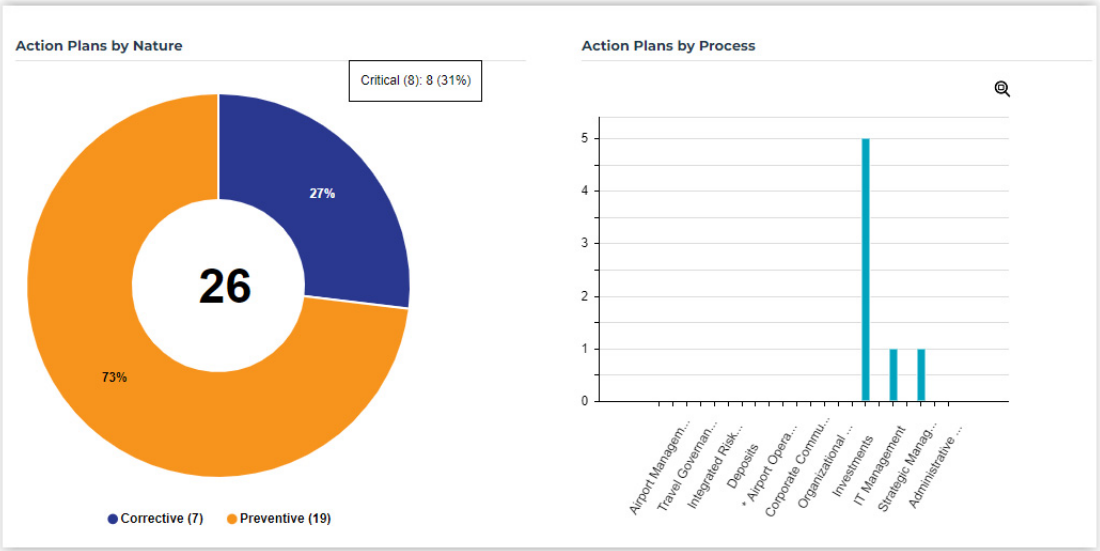
- prevention
- corrective

Action plans by process

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

- x-axis: all processes (business and organizational)
- y-axis: number of action plans linked to each process and sub-process

☛ *If no process is selected, all root processes are taken by default.*

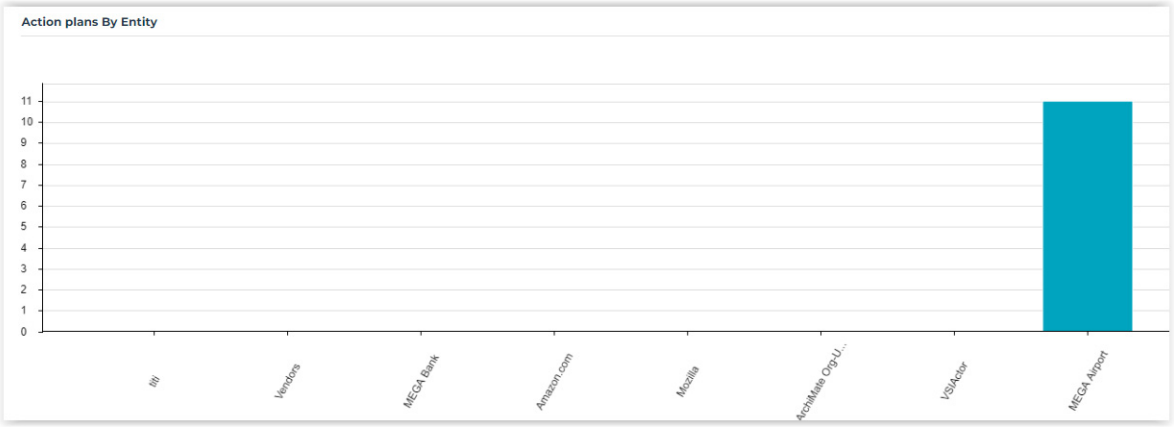


Action plans by entity

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

- x-axis: all entities
- y-axis: number of action plans linked to each entity and sub-entity

☛ *If no entity is selected, all root entities are taken by default.*



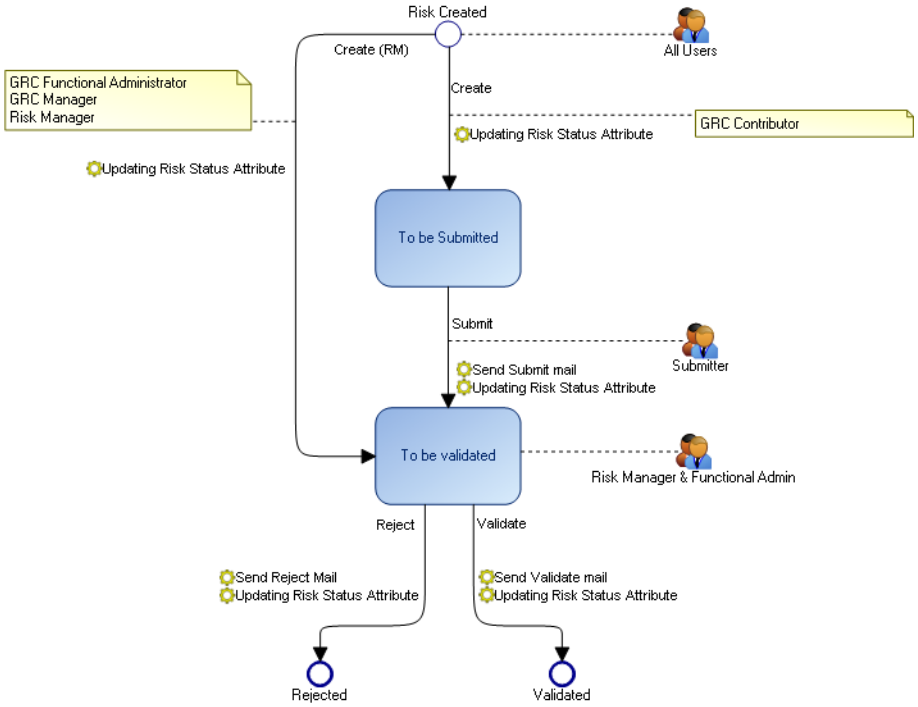
GRC SOLUTION WORKFLOWS

GRC (Governance, Risk & Compliance) activities are performed via ready-to-use workflows.

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

- ✓ Risk Workflows
- ✓ Testing Workflows
- ✓ Action Plan Workflows
- ✓ Incident Workflow
- ✓ Campaign Workflow

RISK WORKFLOWS

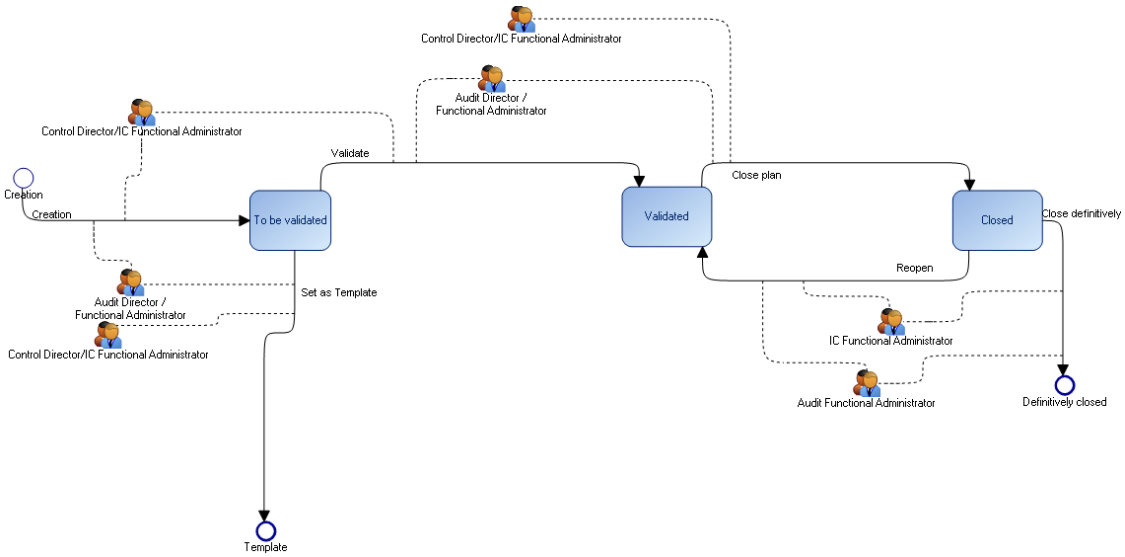


☛ *For more details on the characteristics of risks and risk-related workflow, see Managing Risks.*

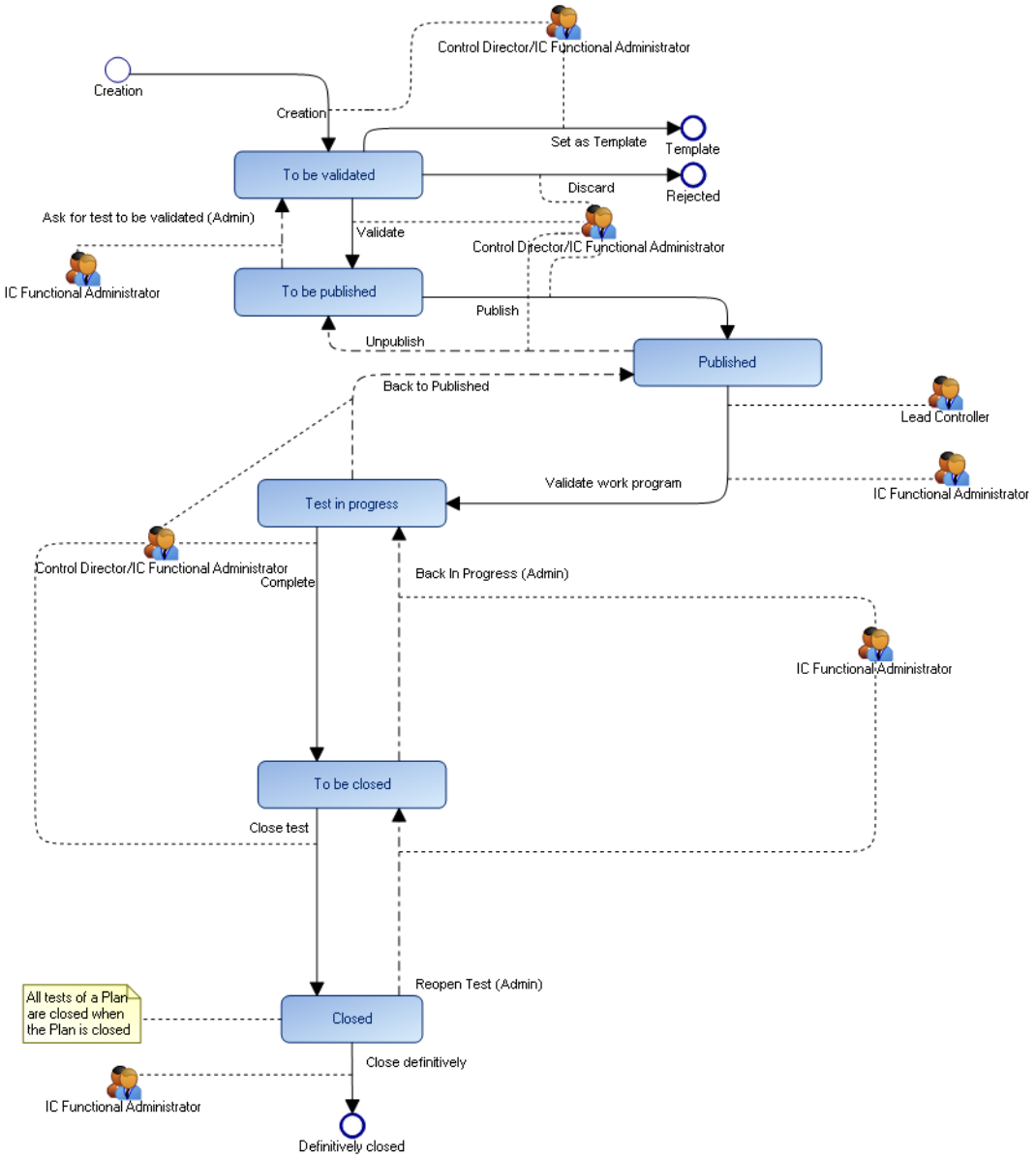
TESTING WORKFLOWS

☛ *For more details on testing, see Control Testing.*

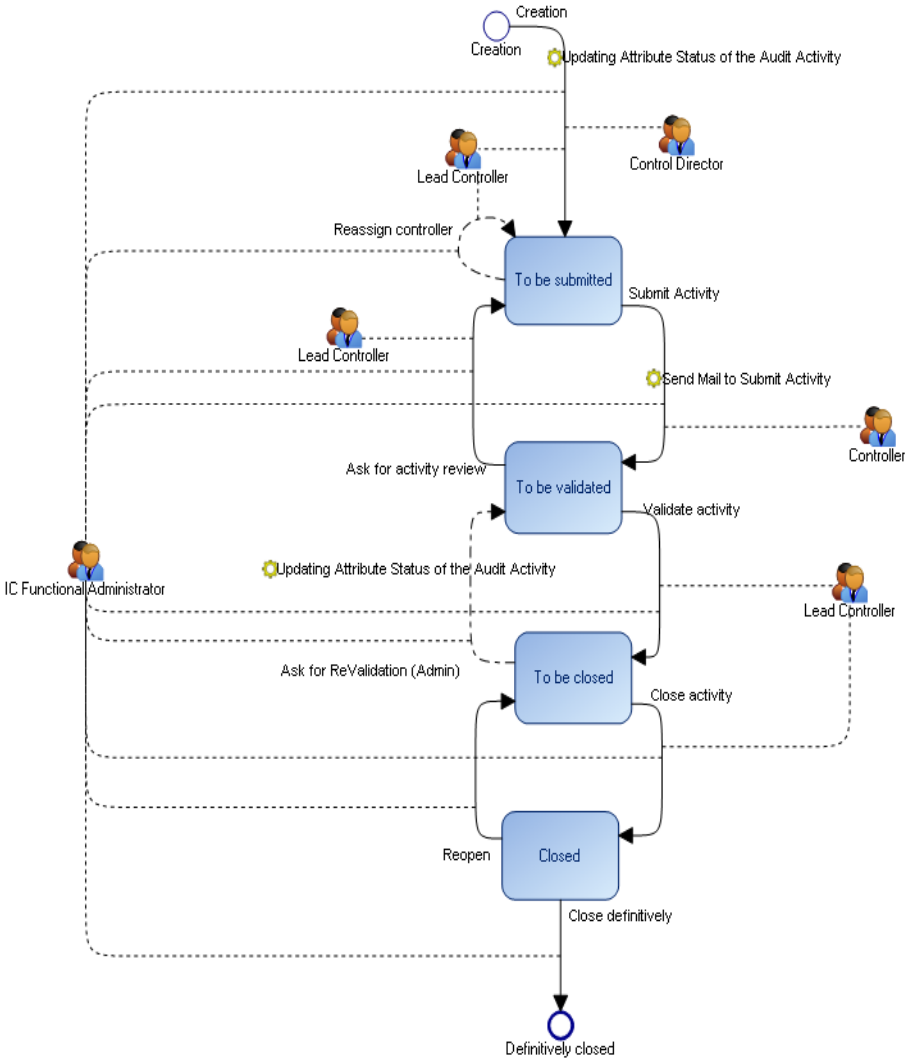
Test Plan/Audit Plan Workflow



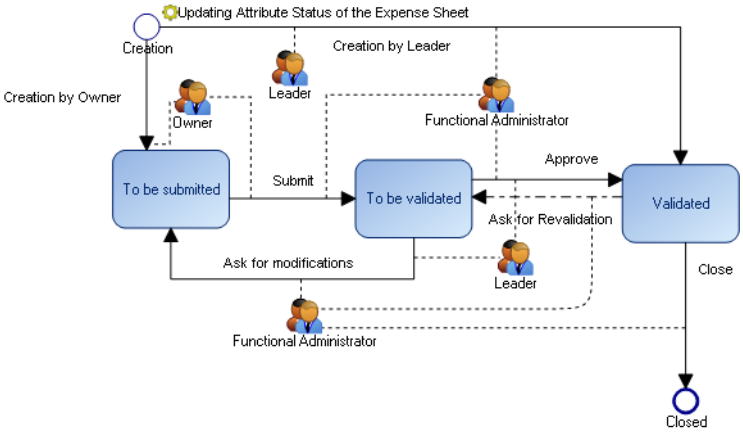
Test Workflow



Test Activity Workflow



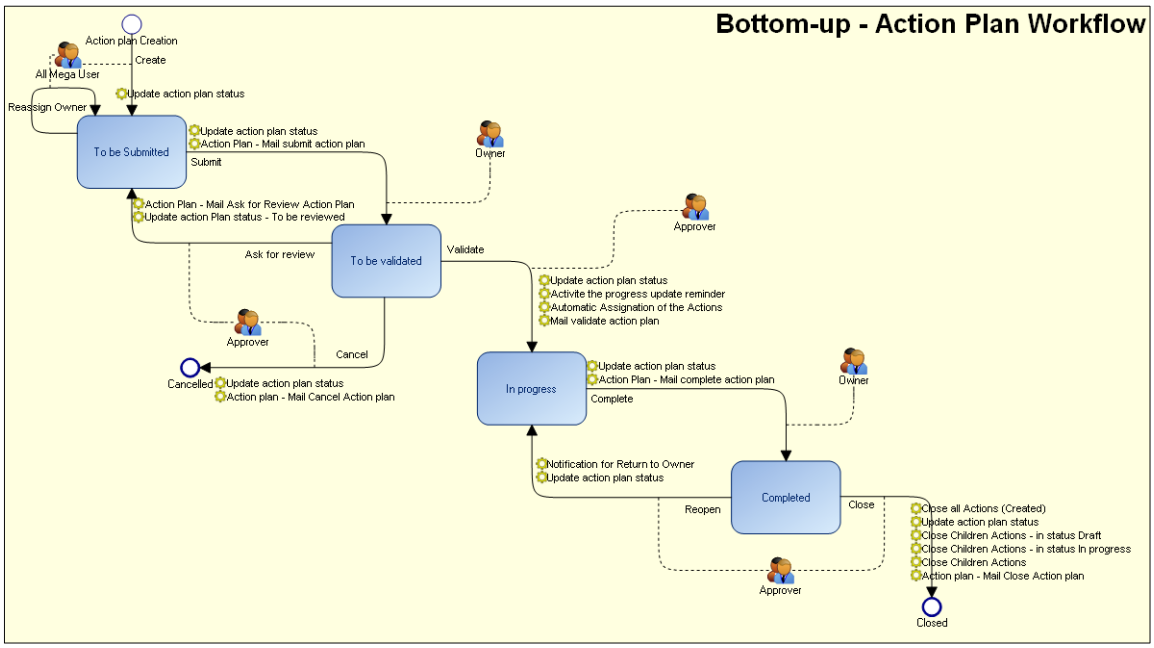
Expense Sheet Workflow



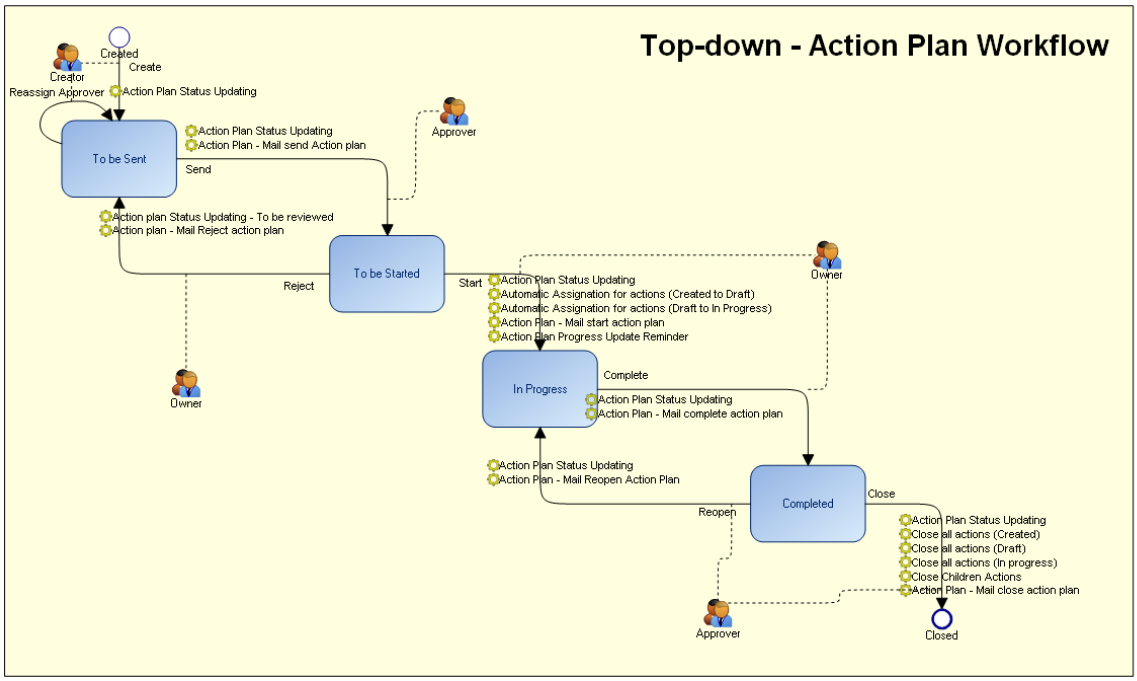
ACTION PLAN WORKFLOWS

☛ *For more information on action plans, see Using Action Plans.*

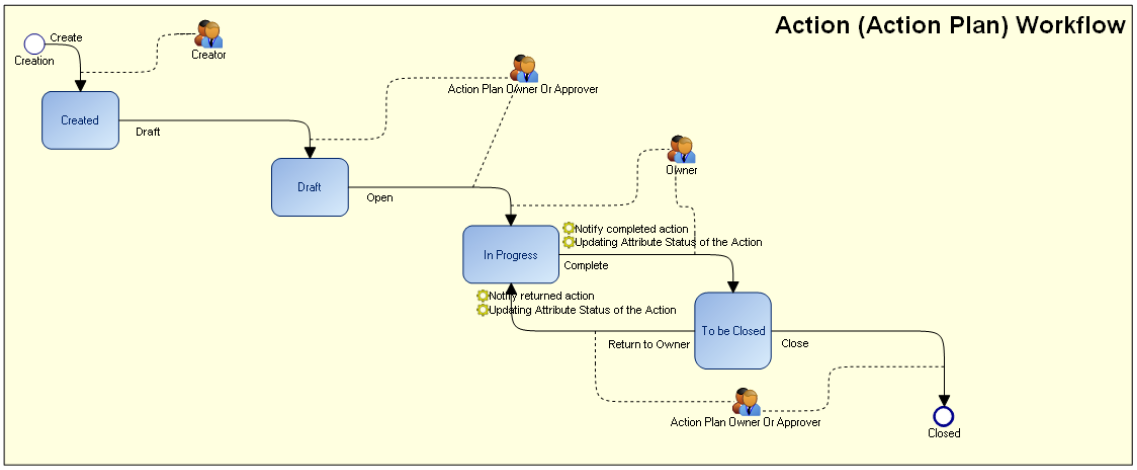
"Bottom-up" Action Plan Workflow

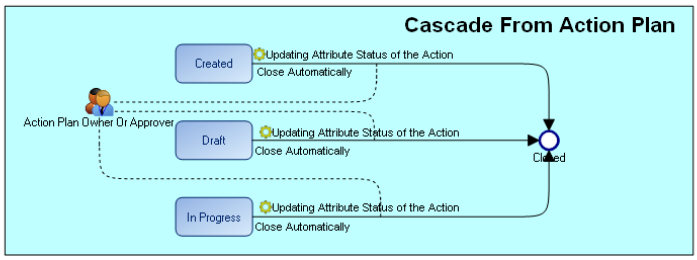


"Top-down" Action Plan Workflow

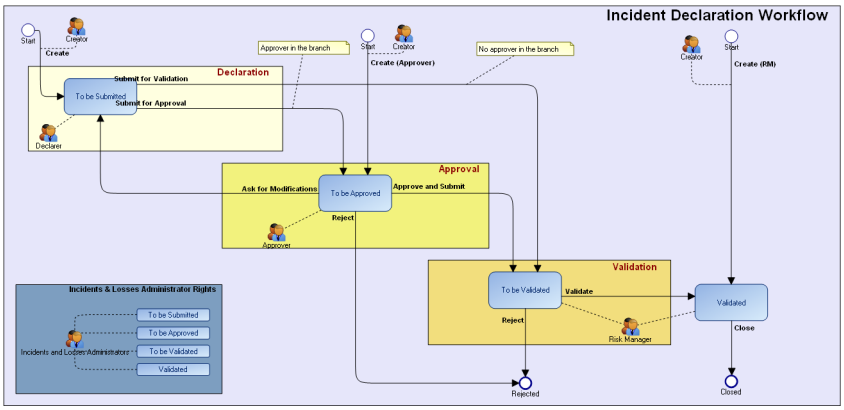


Action Workflow





INCIDENT WORKFLOW



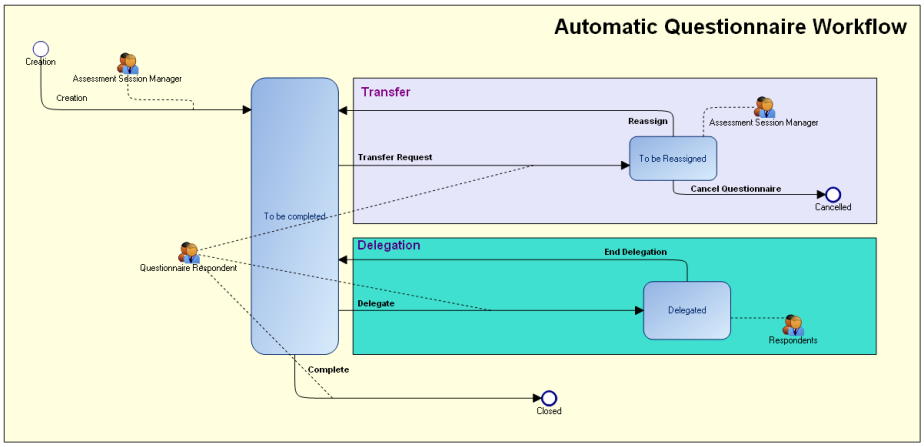
☛ *For more details on incidents, see Incident Management Process.*

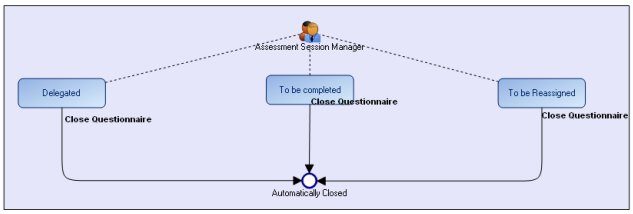
CAMPAIGN WORKFLOW

Assessment Campaign Workflow

See Generic Assessment Workflows.

Execution (Automatic) Campaign Workflow





THE GRC CONTRIBUTOR DESKTOP

A specific desktop enables you to contribute to GRC (Governance, Risk and Compliance) concerns.

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

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

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

PRESENTATION OF THE GRC CONTRIBUTOR DESKTOP

Accessing the GRC Contributor Desktop

To access the GRC Contributor Desktop:

1. See Logging in to Hopex.
2. Login as a "GRC Contributor".

Features Available to the GRC Contributor

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

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

Home Page

The home page enables you to perform the most common tasks on the objects that you work on.

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

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

Dashboard

You can add widgets adapted to various GRC issues.

See:

- Customizing your Dashboard
- Dashboard and Widgets

My Tasks

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

See:

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

Environment

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

- Entities
- Processes
- Applications
- Business lines

For more information, see Viewing your Environment.

Risks

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

This menu enables you to access:

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

For more details on the characteristics of risks, see Risk characteristics.

Controls

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

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

For more information, see Control Characteristics.

Incidents

This menu lists the incidents:

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

> 🕮 *An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.*

For more information, see Managing Incidents.

VIEWING YOUR ENVIRONMENT

To access the objects of your environment:

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

☛ *For a detailed description of these objects, see GRC Environment.*

Processes

🕮 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

🕮 *A process describes how to implement all or part of the process required to make a product or handle a flow.*

For more details, see Managing Process Categories and Processes.

Applications

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

For more details, see Managing Applications.

Business lines

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

For more information, see Managing Business Lines.

Entities

🕮 *Assessment is a mechanism enabling sending of questionnaires to an identified population to obtain assessments (qualitative or quantitative) on identified objects. The assessment is then supplemented by results analysis tools.*

For more information, see Managing Entities.

DASHBOARD AND WIDGETS

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

To add widgets to your dashboard:

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

Widgets for Action Plans

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

Action plans by progress

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

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

Action plan by priority

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

- Critical
- High
- Mean
- Low

Action plans by status

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

- To be started
- Ongoing
- Completed

Action plan dashboard

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

GRC-specific widgets

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

Widgets specific Hopex Internal Audit

See Viewing recommendation widgets.

MANAGING INCIDENTS

An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.

> ☛ *Incidents are available with **Hopex LDC**. For more details, see Collecting Incidents.*

The "GRC Contributor" profile enables you to:

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

> ☛ *For more details, see Managing Action Plans and Actions.*

Creating incidents

To create an incident:

1. See Accessing the GRC Contributor Desktop.
2. In the Quick access part of the home page, click **Create an Incident**.
3. Select the **Declarant's Entity**.
4. Click **Connect** then **OK**.

For more details on incidents, see the **Hopex LDC** documentation. Collecting Incidents.

Accessing incidents

To access your incidents:

❱ In the desktop, click **Incidents** .
The incidents you have created appear.

MANAGING ACTION PLANS AND ACTIONS

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

> ☛ *Action plans are used across all GRC solutions, except in **Hopex Internal Audit** (where recommendations and actions are used instead).*

Context for action plan creation

Two types of workflows are available for action plans:

- top-down
- bottom-up

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

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

- In the "bottom-up" approach, you can create an action plan when you answer a requirement questionnaire.

  > ☛ *You can submit it via the workflow so an approver can validate it.*

- An auditor may detect an issue and asks you to create an action plan in order to remediate it.

  > ☛ *In this case you need to connect the issue to the action plan.*

Accessing Action Plans

To access action plans:

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

Connecting an issue to an action plan

To connect an issue to an action plan:

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

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

Indicating action plan progress

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

To indicate progress:

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

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

Managing actions

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

- specify the actions to take to ensure recommendation follow-up

  ☛ *See Implementing recommendations.*
- ensure actions are correctly implemented

To access your actions:

1. See Accessing the GRC Contributor Desktop.
2. In the navigation bar, click **My Tasks > Action Plans > Actions**.

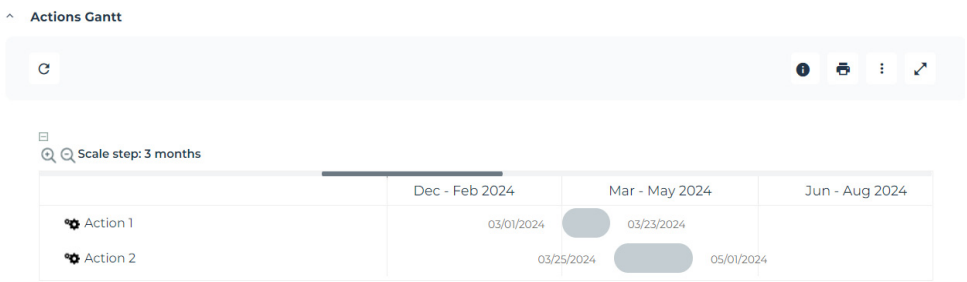
See also Creating an action within the framework of a recommendation.

Viewing action Gantt

Hopex enables you to view the scheduling of actions within a Gantt chart.

To access the action Gantt chart:

1. In the navigation bar, click **My Tasks > Action Plans**.
2. Open the properties of an action plan and select the **Actions** page.
   The action Gantt appears in the lower part of the page:



MANAGING RECOMMENDATIONS

☛ *Recommendations are used within the framework of **Hopex Internal Audit**.*

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

Accessing recommendations

To access your recommendations:

❱ In the navigation bar, select **My tasks > Recommendations**.

Recommendations are classified according to their status:

- Recommendations
- Delayed recommendations

Implementing recommendations

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

As a recommendation owner, you may:

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

For more information on recommendations within the framework of **Hopex Internal Audit**: see Implementing Recommendations.

Creating an action within the framework of a recommendation

To create an action:

1. See Accessing recommendations.
2. In the properties of the recommendation, select the **Action Plan** page.
3. In the **Actions** section, click **New**.
4. Open the properties of the action created.
5. Modify its name if necessary, enter a date limit and an action **Owner**.

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

Submitting an action plan (consisting of recommendations)

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

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

To do this:

1. See Accessing recommendations.

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

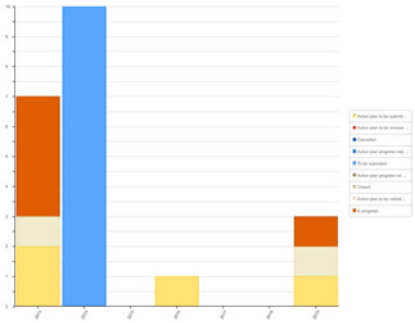
   ☛ *The lead auditor or audit director validates the action plan by return.*

Viewing recommendation widgets

Recommendations by status and year

This bar chart displays recommendations:

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



Recommendations by status and audit

This bar chart displays recommendations:

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

Recommendation Dashboard

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

- Delayed
- On Time

MANAGING QUESTIONNAIRES AND CHECK-LISTS

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

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

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

Accessing Questionnaires

To access questionnaires:

1. See Accessing the GRC Contributor Desktop.
2. In the home page, click on **My Tasks > Questionnaires**.

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

- Questionnaires
- Late questionnaires

Answering a Questionnaire

To complete a questionnaire:

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

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

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

From the questionnaire pop-up menu you can:

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

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

Completing Assessment Check-lists

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

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

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

To complete the check-lists addressed to you:

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

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

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

To make a transfer request:

- Click the icon of a questionnaire and select **Assessment Questionnaire (To Be Completed) > Transfer Request**.
  The questionnaire switches to the "To Reassign" status.

  The manager is informed by e-mail and must reassign the questionnaire to another person.

  ☛ *For more details on control contextualization see Executing Controls.*

CREATING RISKS AND CONTROLS

Creating a risk

To create a risk in the GRC Contributor desktop:

- In the home page, click **Create a risk**.

  ☛ *For more details on users, see Managing Risks.*

Creating controls

To create a control in the GRC Contributor desktop:

- In the home page, click **Create a control**.

  ☛ *For more details, see Managing Controls.*

MANAGING KEY INDICATORS

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

Accessing Key Indicators

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

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

> ☛ *The key indicators you can view are those for which you are requested to enter a value. See Enter a key indicator value.*

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

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

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

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

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

Enter a key indicator value

To enter a key indicator value:

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

Submitting an action plan on a key indicator

To create and submit an action plan:

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

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

Performing a BIA (Business Impact Analysis)

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

☛ *This feature is available with **Hopex BCM**.*

To access a BIA that have been sent to you:

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

TAKING PART IN BUSINESS CONTINUITY PLANS

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

☛ *This feature is available with **Hopex BCM**.*

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

- Business continuity exercises
- Crises

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

Viewing BCPs tested by ongoing exercises

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

To view these:

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

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

Viewing BCPs triggered by ongoing crises

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

To view these:

1. in the navigation tree:
   - (**Hopex GRC**) Select **My Tasks > Business Continuity**.
   - (**Hopex Business Process Analysis**) Select **Continuity > Continuity Tasks**.
2. Expand the **Business Continuity Plans triggered by ongoing crises**.

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

APPENDIX - COMPUTATION RULES

Risk Control Level

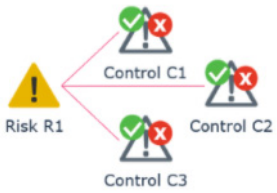
Risk control level enables characterization of control efficiency in mitigating the risk.

Context

When a respondent completes a risk assessment questionnaire, **Hopex GRC** might display a value for Control Level.

A value is displayed if:

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



Computation method

The computation method consists of two steps:

1) Computation of control level average

```
Average Control Level = Total nb. of deficient controls * 25
/ Total number of controls
```

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

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

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

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

Computation example

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

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

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

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

Inherent risk

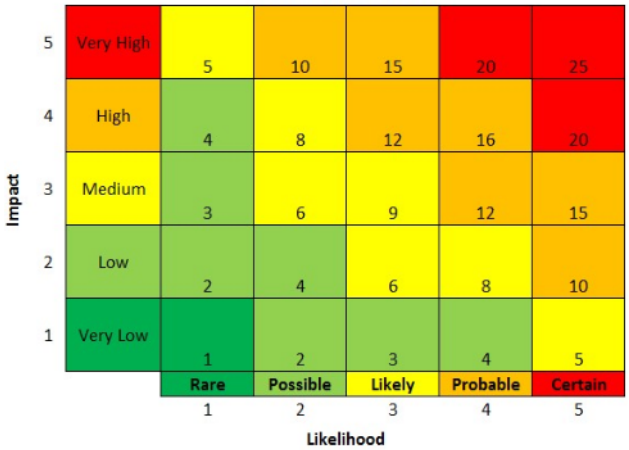
The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact of this risk.

Computation method

Inherent risk = Impact x Likelihood

Possible values

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



Residual Risk

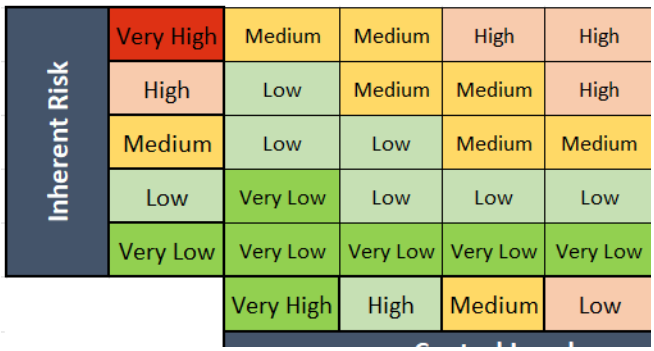
The residual (or net risk) indicates the risk to which the organization remains exposed after management has processed the risk.

Computation method

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

Possible values

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



RTO (Recovery Time Objective) Computation

📖 *The Recovery Time Objective (RTO) determines the maximum tolerable amount of time it takes to bring critical systems back online, possibly in a Degraded Mode. It is related to downtime, representing target time following an incident for Product or service delivery resumption, or Activity resumption, or Resources recovery.*

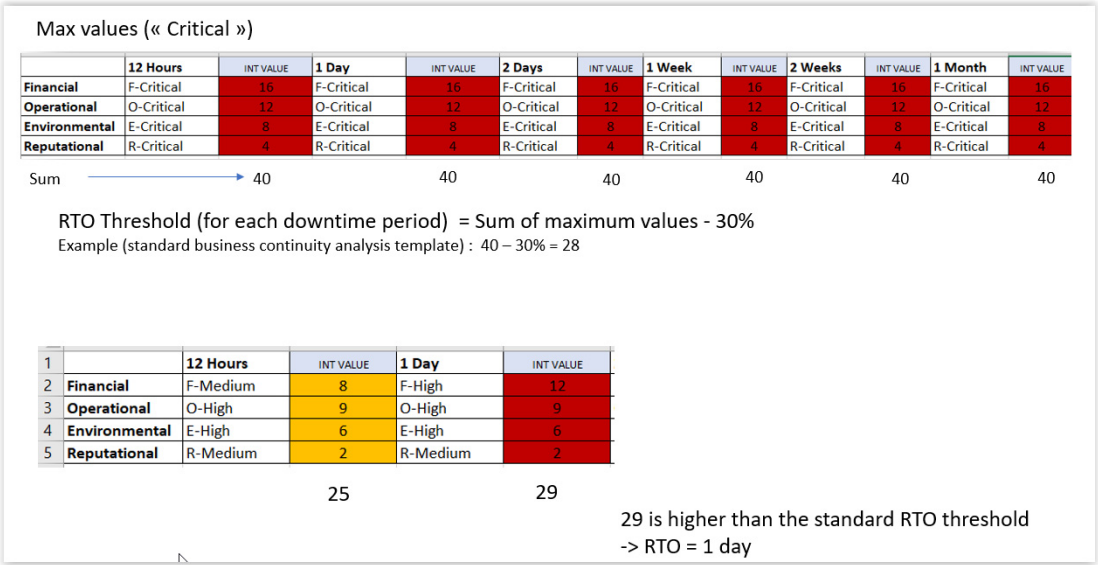
☛ *For more details, see Viewing a BIA Computed Results.*

The algorithm:

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

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

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



Max values (« Critical »)

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

RTO Threshold (for each downtime period) = Sum of maximum values - 30%

Example (standard business continuity analysis template) : 40 – 30% = 28

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

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

Business Impact Computation

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

☛ *For more details, see Defining a Business Impact Analysis.*

The business impact is computed as follows:

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

GRC GLOSSARY

action

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

action plan

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

activity program

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

aggregation method

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

aggregation period

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

aggregation rule

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

aggregation schema

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

application

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

article (of regulatory framework)

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

assessed characteristic

An assessed characteristic defines what the assessment seeks to assess. It can be associated with a MetaClass, and more specifically with one of its MetaAttributes, for example: Risk MetaClass, MetaAttribute: Criticality.

assessment

Assessment is a mechanism enabling sending of questionnaires to an identified population to obtain assessments (qualitative or quantitative) on identified objects. The assessment is then supplemented by results analysis tools.

assessment campaign

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

assessment freshness

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

assessment session

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

assessment template

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

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

audit

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

audit activity

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

audit program

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

audit theme

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

business document

A business document is a document whose content is independent from the HOPEX repository. This document can be MS Word, MS Powerpoint, or other files. A report (MS Word) generated on an object can become a business document.

business line

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

business policy

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

calendar

A calendar is divided into calendar periods.

calendar

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

calendar period

A calendar period is a division of a calendar.

central currency

Central currency is the currency adopted as reference currency.

company

A company is a legal entity.

Compliance rate

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

contract

A contract is a written agreement between the organization and a vendor.

control

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

control assessor

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

control directive

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

Control level

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

control level

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

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

control redundancy

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

control type

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

data center

A data center is a physical site that groups together IT facilities responsible for storing and distributing data through an internal network or via Internet access.

database

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

department

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

deployed server

A (deployed) server is a computer on which applications are run.

enterprise stage

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

entity

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

entity

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

execution rate

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

facility

A facility is a model of site of interest for the enterprise (for example: factory, outlet).

findings

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

forecast risk

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

gain

A gain is the positive financial consequence of an incident.

incident

An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.

incident approver

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

incident declarant

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

indicator

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

indicator interpretation logic

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

Indicator status

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

inherent risk

The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact.

internal audit

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

key indicator

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

key indicator category

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

library

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

local currency

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

loss

A loss is the negative financial result of an event.

macro-incident

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

materialized risk

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

metric

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

near-miss

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

objective

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

operation

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

period

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

person

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

policy framework

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

process

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

process category

A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.

product

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

profile

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

provision

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

questionnaire

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

questionnaire template

A questionnaire template represents definition of questionnaire content.

recommendation

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

recovery

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

regulation framework

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

regulation or policy

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

regulatory framework

A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), or standards.

requirement

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

residual risk

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

respondent

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

risk

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

risk and control system

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

risk appetite

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

Risk assessor

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

risk consequence

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

risk factor

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

Risk Manager

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

Risk type

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

role

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

scoring rule

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

section (of regulatory framework)

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

server

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

site

A site is a geographical location of an enterprise. Examples: Boston subsidiary, Seattle plant, and more generally the headquarters, subsidiaries, plants, warehouses, etc.

software installation

A software installation on a site offers a set of functionalities to different populations of users.

software technology

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

steering calendar

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

to automatically trigger assessment sessions at regular intervals,...

test

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

test plan

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

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

vendor A vendor is a external org-unit of "Vendor" type.

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

Hopex Internal Control

User Guide

Hopex Aquila

CONTENTS

Contents

About Control Management

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

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

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

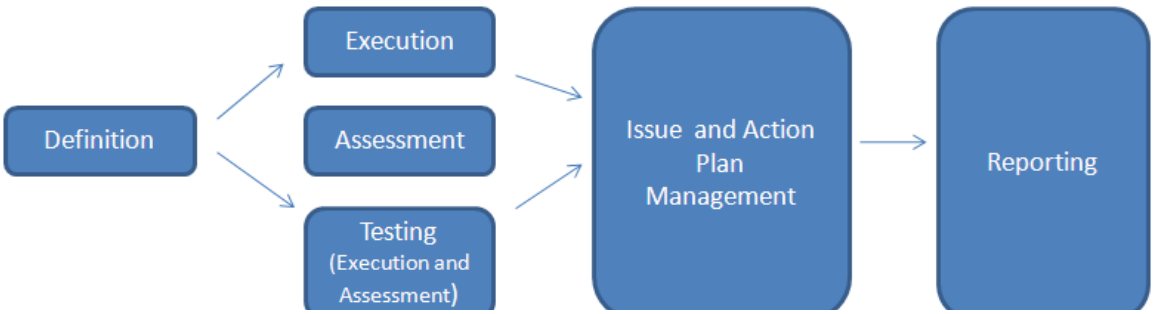
- ✓ Internal Control Process
- ✓ Control Management Profiles

INTERNAL CONTROL PROCESS

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

Hopex Internal Control covers the different phases of internal control:

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



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

Execution and assessment of controls can be carried out independently.

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

Control register definition

Hopex Internal Control allows internal control managers to:

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

See Managing Controls.

Control Execution

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

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

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

See Executing Controls.

Control Assessment

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

- assessment campaigns via questionnaires
  See Assessment Campaigns.
- direct assessment
  See Assessing Controls.
- control tests organized by the internal control department
  See Control Testing.

Issue and Action Plan Management

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

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

See Managing Issues and Action Plans.

CONTROL MANAGEMENT PROFILES

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

Profiles	Desktop	Tasks
Internal Control Director (Or GRC manager)	Hopex GRC	- Have all rights on workflows, objects and menus of the solution - Validate campaigns - Prepare test plans - Validate action plans
Internal Controller (Or GRC manager)	Hopex GRC	- Define controls - Prepare campaigns - Execute tests (create work programs, create issues and action plans) - Validate and follow up action plans
GRC Contributor (Lite)	GRC Contributors	- Complete control execution check-lists - Answer assessment questionnaires - Define and create action plans (and create issues) See The GRC Contributor Desktop.

☛ *For further details, see Accessing the GRC Desktop.*

MANAGING CONTROLS

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

CREATING CONTROLS

To create a control:

1. In the navigation bar, click **Controls**.
2. Click **New**.

   ☛ *You may also create a control from the home page (**Quick access > Actions > Create a Control)**.*

3. In the creation wizard, enter:
   - the **Name**
   - **Control Nature**
   - **Execution Mode**
   - a **Description**.

     ☛ *For more details on characteristics, see Control Characteristics.*

The control created appears in the list of controls.

You can specify the various characteristics from the properties page.

CONTROL CHARACTERISTICS

☛ *To access controls, see Accessing Controls.*

General characteristics

Code

The code enables unique identification of the control.

Key control

Enables to define whether the control is major or not.

Status

- Draft
- Validated

☛ *Status must be entered manually.*

Owner

The control owner is by default the control creator.

☛ *The control owner has no particular task to perform.*

Control nature

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

- Corrective
- Detective
- Preventive

Execution mode

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

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

Operational cost

This characteristic enables indication of a control cost assessment.

Description and Control objective

You can enter a comment and/or text describing the objective in setting up the control.

Control Overview

☛ *See Accessing Controls.*

The **Overview** page gives access to:

- A control card, which gives an overview of the main control characteristics

  ☛ *For more details, see Card of an Object in the "Platform - Common Features" section.*

- Computed information in the form of a dashboard

Identification

An identification card summarizes the main control properties:

- **Code**

  ☛ *See Code.*

- **Description**

  ☛ *See Description and Control objective.*

- **Owner**

  ☛ *See Owner.*

- **Execution mode**

  ☛ *See Execution mode.*

- **Nature**

  ☛ *See Control nature.*

- **Key**

  ☛ *See Key control.*

Dashboard

Last assessment

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

Latest compliance rate

The compliance rate relates to control execution check-lists. For more details on this functionality, see Executing Controls.

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

Open issues

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

For more details, see Managing Issues and Action Plans.

Control level

Control Level is related to control assessment. For more details, see Displaying the Results of Control Assessment.

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

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

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

Responsibilities concerning Controls

See also: Accessing Controls.

Hopex GRC enables definition of responsibilities of each participant related to a control via the RACI matrix:

- Responsible
- Accountable
- Consulted
- Informed

Responsibility levels

RACI responsibility levels are as follows:

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

Specifying control responsible users

In the framework of control assessment and execution, questionnaire respondents are ***Responsible*** users of the control.

☛ *See the section corresponding to the respondent logics in the prerequisites to control assessment. Pre-requisites to Control Assessment.*

☛ *See also: Assessment Campaigns.*

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

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

   ☛ *To access controls, see Listing Controls.*

2. Select the **Responsible** tab.
3. Click the **New** button.
4. Select a person in the drop-down list provided.

   ☛ *The business role "Control Responsible" is specified by default.*

5. (optional) Select the entity the person is responsible for.
6. Click **OK**.

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

   ☛ *You have the possibility to connect several responsible users.*

Scope of a Control and Associated Risks

To specify the scope of a control:

- In the **Characteristics** page of the control properties, expand the **Scope** section.
  You can connect several object types:
  - Process categories
  - Processes
  - Operations
  - Entities
  - Applications
  - Accounts
  - Types of control

To specify risks for a control:

- In the **Characteristics** page of the control properties, expand the **Risks** section.

Regulatory and Business Policy Enforcement

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

1. See Accessing Controls.
2. In the **Characteristics** page of the control properties, expand the **Regulatory and Policy Enforcement** section.

Several tabs enable you to view associated objects:

- Control Directives

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

- Articles

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

- Business Policies

  ☛ *For more details, see Managing Compliance.*

Action Plans for Controls

To specify action plans on a control:

❱ In the control properties, select the **Action Plans** page.

You may:

- define action plans directly on the control
- view action plans on issues associated to the control

  ☛ *For more details, see Managing Issues and Action Plans.*

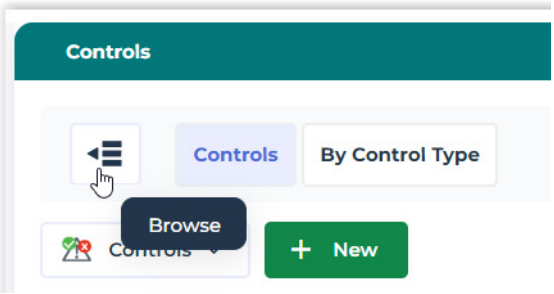
Reports Related to Controls

See Control Environment Report.

Browsing a Control Environment

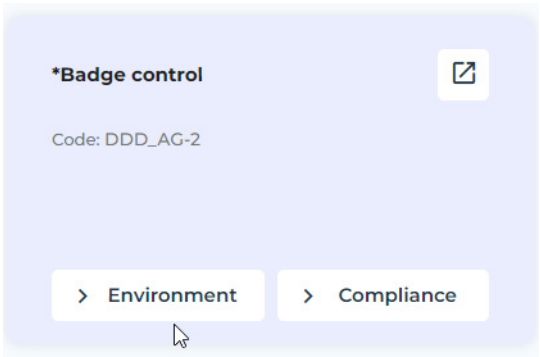
To browse the objects of the control environment:

1. See Accessing Controls.
2. In the list of controls, click **Browse**.



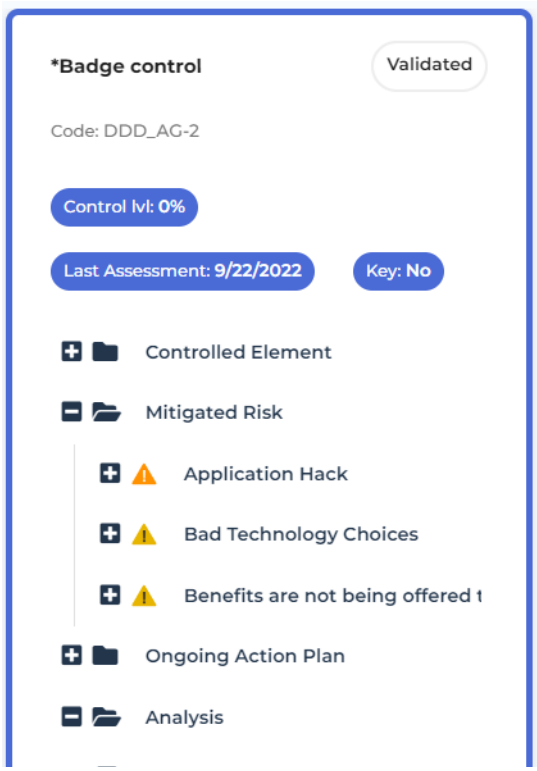
A card is available for each control.

3. Hover the mouse over a card and click **Environment**.



The objects of the control environment are displayed in trees. They form the control extended scope.

- Objects of the environment
- Objects of the compliance environment / regarding regulation enforcement.



ACCESSING CONTROLS

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

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

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

Listing Controls

To list all controls:

- In the navigation bar, click **Controls**.

Accessing Orphan Controls

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

1. See Listing Controls.
2. From the drop-down list, select **Orphan Controls**.

> ☛ *To define a control appropriately, connect it to a risk and make sure you have defined the risk scope.*

Accessing Controls by Incidents

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

1. See Listing Controls.
2. From the drop-down list, select **Controls with Incidents**.

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

CONTEXTUALIZING CONTROLS

The same control can be assessed in the framework of different contexts (for example process categories, processes or entities).

To enable this multiple assessment, you must "contextualize" controls, that is connect them to context objects.

You must ***connect controls to risks which are connected to process categories, processes or entities***.

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

- *Connect process categories or processes to entities of the organization.*
- *Connect controls to process categories and processes.*

ASSESSING CONTROLS

Controls are assessed in terms of design/efficiency.

Assessment can be made:

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

Hopex GRC also enables internal controllers and auditors to answer questionnaires on site. For more details, see Control Testing.

☛ *This chapter explains how to start assessments. To configure these, see Assessment Templates in the **Hopex Power Studio** - Assessment documentation.*

Control Assessment Types

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

Direct Assessment or via Campaign

Direct assessment

The GRC Manager can specify characteristic values:

- From the control properties page: see Assessing a Control.
- From a multiple assessment table: see Assessing Multiple Controls Simultaneously.

Assessment By Campaign

Characteristic values can be collected via an assessment questionnaire sent to appropriate recipients: see Starting an Assessment Campaign

Controls Assessment Templates

Hopex enables you to assess controls from two different perspectives:

- Control Assessment by Entity
- Control Assessment by Entity and Regulatory Framework.

☛ *See Pre-requisites to Control Assessment for more information on these assessment templates.*

PRE-REQUISITES TO CONTROL ASSESSMENT

Control Assessment by Entity

The "Control Assessment" template enables to assess control in the context of entities and process categories/processes based on the following criteria:

- Design
- Effectiveness

Assessment contexts

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

Prerequisites

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

Check that you have:

- connected controls to process categories and processes (indirectly via risks, or directly)
- connected process categories and processes to the organization entities (directly or indirectly via the process category)

  ☛ *See Contextualizing Controls.*
- defined respondents.

  ☛ *See:*

  - *Pre-requisites to Control Assessment*
  - *Specifying respondents*
- specified an e-mail for each respondent.

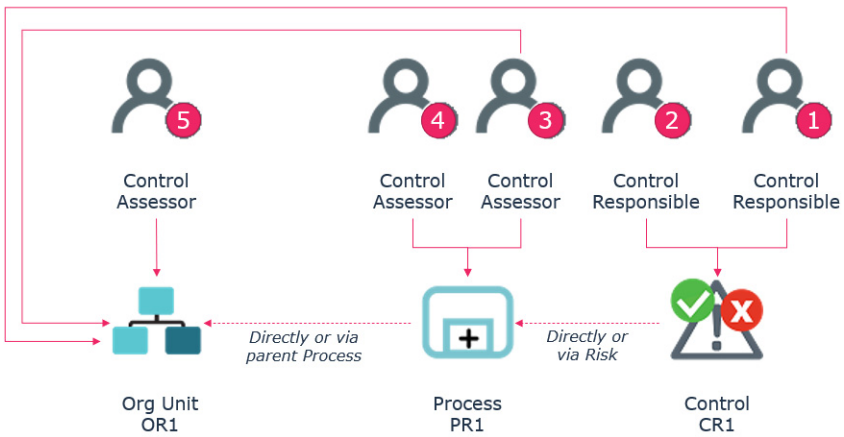
Respondent definition logics

Respondents to control-related questionnaires can be defined on:

- entities
- controls connected to entities (via a risk or indirectly via the parent process)
- controls connected to processes (via a risk or directly)

  ☛ *See also Contextualizing Controls.*

Hereafter the logical order used to compute respondents on controls:



The control respondent is computed in the following order:

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

Specifying respondents

To specify respondents, see:

- Specifying control responsible users.
- Specifying responsibilities
- Specifying responsibilities within an entity

Control Assessment by Entity and Regulatory Framework

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

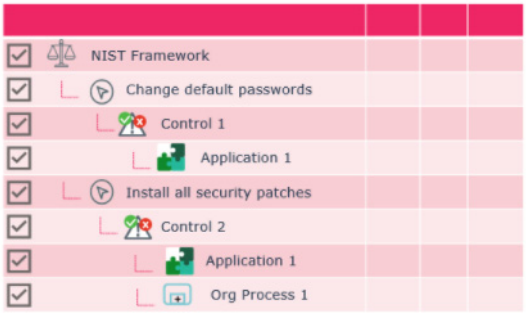
Assessment contexts

Controls are assessed in the context of processes and applications.

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

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

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



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

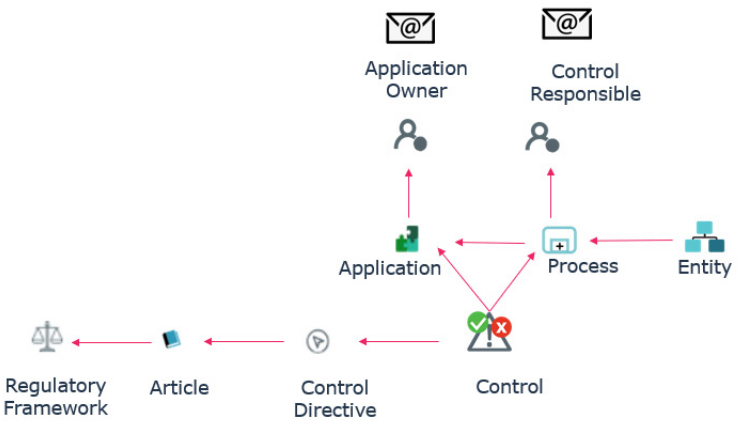
☛ *Controls connected to an application non connected to a process are excluded.*

Prerequisites

Check that you have:

- connected controls to control directives.
- connected controls to processes or applications.
- defined respondents.
  - for applications: the application owner
  - For processes: the control responsible user

    ☛ *See Specifying responsibilities.*
- specified an e-mail for each respondent.



Possible use

This assessment template can bu used with the framework of:

- control assessment campaigns
- multiple direct assessment

> ☛ *Specific reports enable to follow-up the compliance process progress. See IT Regulatory Compliance Reports.*

CONTROL DIRECT ASSESSMENT

Hopex GRC enables assessment of controls in terms of design and efficiency:

You can assess controls:

- Directly
- Through questionnaires sent to identified recipients.

> ☛ *For assessment by questionnaire, see Assessment Campaigns.*
>
> ☛ *See also: Pre-requisites to Control Assessment.*

Direct Assessment Context

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

- in the properties of each control: Assessing a Control.
- globally: Assessing Multiple Controls Simultaneously

This is an "expert view" assessment.

> ☛ *You can assess controls for which you have editing rights.*

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

> ☛ *For more details on control contextualization see also Contextualizing Controls.*

Assessing a Control

> ☛ *Before assessing a control, you need to ensure it has been contextualized in an appropriate way. For more details, see Contextualizing Controls.*

To directly assess a control:

1. Open the properties of a control.
2. Select the **Assessment** page then click **Perform Assessment**.

   > ☛ *If the control has not been properly contextualized, a warning is displayed (a control must be connected to a process, in turn connected to an entity).*
3. In the wizard that appears, select the context(s) to be included in the control assessment.
4. Click **Next**.
   You can now select values that characterize this control (contextualized) in terms of:
   - design
   - effectiveness

   > ☛ *Other questions can be asked if your administrator has configured the questionnaire supplied as standard.*

5. In the **Control Design** and **Effectiveness** fields, indicate whether the control is:
   - Pass
   - Fail

   ☛ *Values are applied to all previously selected assessment nodes.*
6. Specify the measure date in the calendar.
   By default this is today's date. You can select a date earlier than today's date.
7. Click **OK**.
   Control measures are created for each assessment node (ie. the control in a particular context).

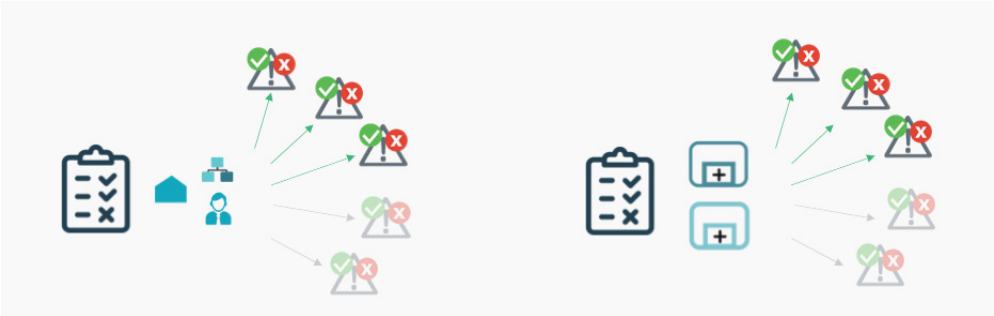
You can create several measures on different dates in the same way.

Assessing Multiple Controls Simultaneously

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

☛ *An assessment node comprises:*

- *an object to assess*
- *one or several context objects (entities, processes, operations), if necessary*



To assess multiple controls simultaneously:

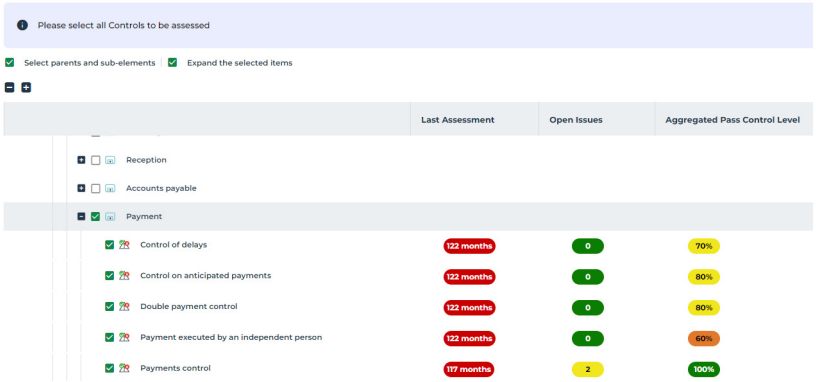
1. In the navigation bar, click **Assessment > Direct Assessment > Control Multiple Assessment**.
2. Click **New Assessment**.
3. In the window that appears, select the assessment template:
   - "Control assessment"
   - "Control Assessment by Entity and Regulatory Framework"

   ☛ *For more details, see Controls Assessment Templates.*

4. Select the context objects of interest.

   ☛ *If you chose the "Control assessment" template, a tree appears. A control is assessed in the context of elements of the branch from the control up to the root.*

   Information is given in columns to help you select the controls to assess.



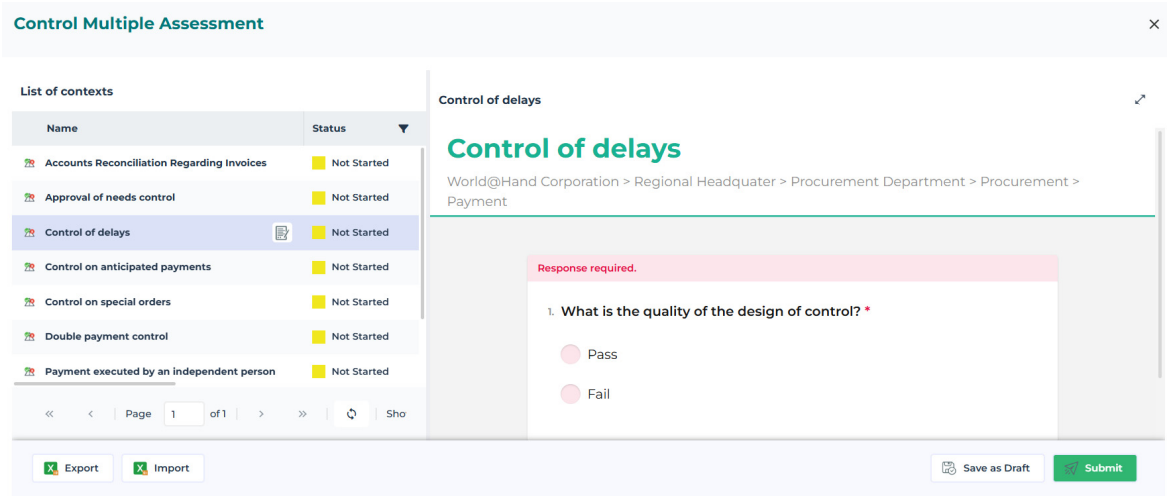
In the above example, if you select the "Payment" process, all controls and context objects located at a lower level are selected, as well as all parent context objects up to the tree root.

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

5. Click **Next**.
   A summary of the assessment appears, enabling you to have an overview of the objects you are going to assess.

6. Click **OK**.
   The list of controls to be assessed in a particular context appears.

7. Enter the control **Design** and **Effectiveness** quality level:
   - Operational
   - Unsatisfactory



8. After answering questions, click **OK**.

   ☛ *You can also choose to close the questionnaire to come back to it and resume the assessment later on.*

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

ASSESSMENT CONTROL RESULTS

Displaying the Results of Control Assessment

To display the results of assessments performed on a control:

- From the control register, select the **Assessment** page of the control properties.

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

See also: Assessment Result Computing Mode.

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

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

Analyzing Control Assessment Results

Instant reports

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

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

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

Dedicated analysis reports

In addition to instant reports, **Hopex GRC** provides dedicated report templates that facilitate the analysis of the assessed controls.

Assessment Result Computing Mode

Metaattribute	Computed / Not Computed	Explanations
Control Design (IC)	Computed through the [Internal Control - Control Attributes] macro	- if ***assessment node***, value computed from the assessed characteristic "Control Design" (IC). - if ***aggregation node***, value computed from the assessed characteristic "Average percentage of Pass Control Level".
Control Effectiveness (IC)	Computed through the [Internal Control - Control Attributes] macro	- if **assessment node**, value computed from the assessed characteristic "Effec-tiveness". - if ***aggregation node***, value computed from the assessed characteristic "Average percentage of Pass Control Level".
Control level (IC)	Computed through the [Internal Control - Com-puted Control Attributes] macro	Rounded result obtained from the formula: Control Design (IC) * Control Effectiveness (IC)

☛ *For more details on aggregation, see Aggregation Schemas.*

EXECUTING CONTROLS

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

Controls are executed in their context, by process and entity. They are presented in the form of check-lists. These check-lists are questionnaires presenting questions on each control.

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

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

- ✓ Preparing Control Execution
- ✓ Continuous Control Assessment Template
- ✓ Creating an Execution Campaign
- ✓ How an Execution Campaign Works
- ✓ Completing Control Execution Check-Lists
- ✓ Managing Execution Check-Lists
- ✓ Check-List Results
- ✓ Control Execution Reports

PREPARING CONTROL EXECUTION

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

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

Defining controls Steps

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

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

For more details on question types, see Question Types.

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

To create questions on a control:

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

An edition wizard appears, in which you can create control steps (questions):

For more information on how to use it, see Defining Questionnaire Templates.

If control steps have been previously defined as a template, the wizard offers to:

- create new control steps, or
- initialize control steps from an existing template.

> ☛ *For more details, see Creating Control Steps from an Existing Template.*

Make Control Steps Reusable

After creating control steps, you may decide to promote them as a template to be able to reuse them.

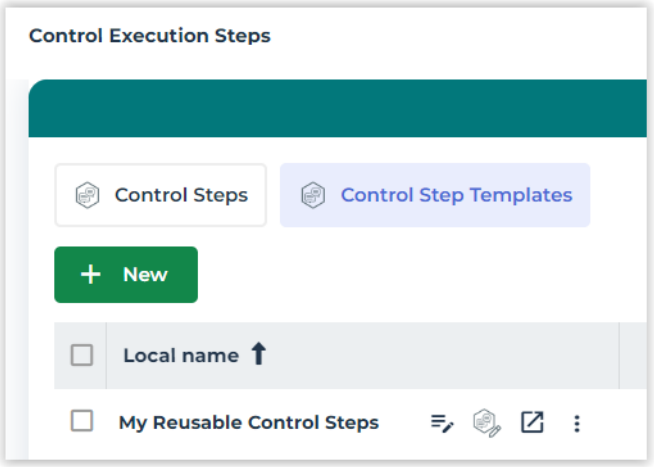
To be able to reuse control steps:

1. Define control steps.

   > ☛ *See Defining controls Steps.*

2. Click **Save as template**.
3. Name your reusable control steps.

Once the "template" has been created, you may view it in **Assessment > Control Execution Steps > Control Step Templates**.



From now on, when you create control steps, a wizard offers you the possibility to create them from scratch or to initialize them from an existing template.

> ☛ *If you no longer want to have these control steps as possible templates, in the **Execution** page of the control, click **Demote as template**.*

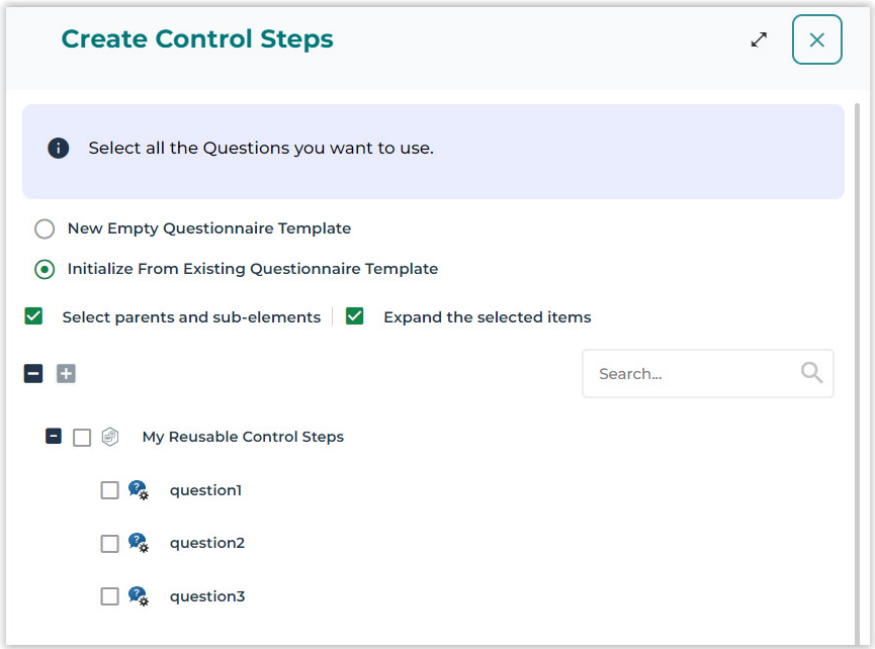
Creating Control Steps from an Existing Template

To initialize control steps from an existing template:

1. See Defining controls Steps.

2. Click **Initialize from an existing template**.

☛ *Select the questionnaire template as well as the questions to include (you may select only some of them).*



☛ *The available control step templates can be found in **Assessment > Control Execution Steps**.*

Defining Steering Calendars on Controls

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

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

To create a steering calendar, see Managing Steering Calendars.

Specifying a control steering calendar

To specify a steering calendar:

1. In the control properties, select the **Execution** page.
2. Ensure you have properly created a questionnaire template.
3. Select an **Execution Frequency**.

☛ *This field is for information only.*

4. Select a **Steering Calendar**.
   Different steering calendars exist for different execution periodicities:
   - daily
   - monthly
   - weekly

Modifying a steering calendar after campaign creation

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

To ensure all check-lists are properly scheduled:

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

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

Defining the Total Population and Sample Size

☛ *This step is optional.*

You can define:

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

  ☛ *This information is optional.*

  For example:

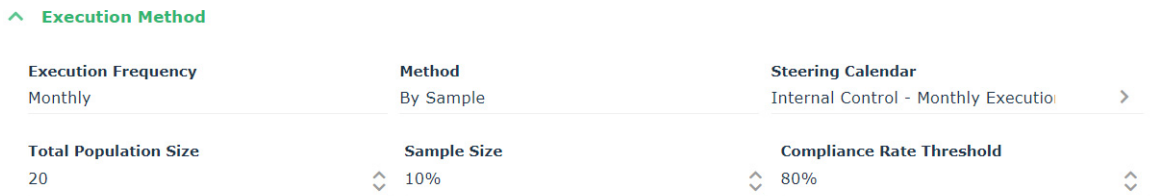
  - **Control**: "Check the contract signature"
  - **Total population**: 20 (20 contracts)
  - **Sample size**: 10% (2 controls are checked)

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

To specify the total population and sample size:

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

3. Specify the following information:



☛ *The **Compliance threshold** enables to compute the execution result.*

The control is "Passed" if the compliance rate is greater than or equal to the compliance threshold.

Defining Respondents

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

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

The logics behind respondent definition is the same as for control assessment by entities. See Control Assessment by Entity.

Connecting Controls to Entity Processes

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

To connect controls to processes, see Contextualizing Controls.

CONTINUOUS CONTROL ASSESSMENT TEMPLATE

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

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

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

Respondents

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

Check-lists sent

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

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

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

☛ *For more details, see Defining the Total Population and Sample Size.*

```
For example:
If total population size = 10 and if sample size = 20%
Then the number of assessment nodes = 10*0.2 = 2
```

Answer computation

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

☛ *For more details on definition of questionnaire answers, see Question Types.*

Aggregated results

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

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

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

CREATING AN EXECUTION CAMPAIGN

To create an execution campaign:

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

   ☛ *The "Continuous Control Execution" assessment template is selected by default. For more details, see Continuous Control Assessment Template.*

   You are now going to define the way of specifying your campaign scope.
3. In the field **Define scope via a tree**, select:
   - **Yes**: a tree enables to define the scope in a very precise way, but it does not allow to take into account the controls added after campaign creation.

     ☛ *If you choose this option, see Defining scope via a tree.*
   - **No**: a **Root entity** field is displayed.

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

   ☛ *The campaign **Begin Date** marks the start of the execution campaign.*
5. Click **Next**.
   The campaign summary appears.

   ☛ *See Displaying the Execution Campaign Summary.*
6. Click **OK**.
   The campaign appears in the list. It is started automatically:
   - on the begin date specified on the campaign
   - at the time indicated on the steering calendar

   ☛ *See Consulting Execution Campaign Schedule.*

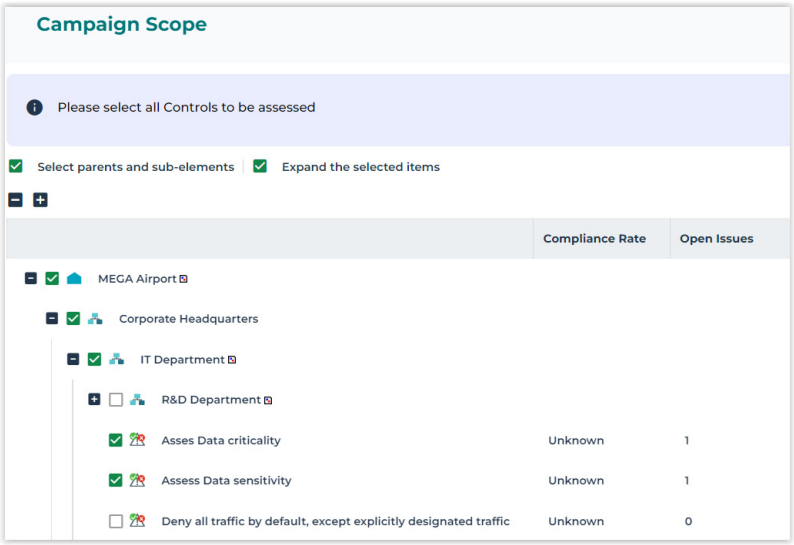
Defining scope via a tree

To define the campaign scope:

1. See Creating an Execution Campaign.
2. Display the wizard that enables to define the scope.

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

     The compliance rate is the percentage of "Pass" controls.
   - **Open Issues** (number)



Displaying the Execution Campaign Summary

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

General information (Overview)

Number of:

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

Contexts

Contexts appear in the form of a process and entity hierarchy

Respondents

Respondents execute controls.

☛ *For more details on control responsibilities, see Responsibilities concerning Controls.*

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

Assessed objects

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

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

How an Execution Campaign Works

Control Execution Periodicity

An execution campaign groups several execution sessions.

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

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

For example:

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

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

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

See also: Examples of Session Automatic Launch.

Examples of Session Automatic Launch

Execution sessions are launched according to the following information:

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

> ☛ *For more details on steering calendars, see Defining Steering Calendars on Controls.*

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

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

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

Example 1

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

Example 2

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

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

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

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

Example 3

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

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

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

Consulting Execution Campaign Schedule

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

1. In the navigation bar, select **Assessment > Campaigns > Execution Campaigns**.
2. Open the properties of the execution campaign and select the **Gantt** page.
   The list of timespots defined by the steering calendar appears.

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

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

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

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

Defining Reminders

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

Modifying reminders provided as standard

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

To modify the reminders provided as standard:

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

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

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

Deactivating reminders

To deactivate reminders:

❱ Empty the cells of the reminder definition table.

Closing Check-lists

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

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

To do this:

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

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

COMPLETING CONTROL EXECUTION CHECK-LISTS

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

☛ *For more details, see Managing Questionnaires and Check-lists.*

Accessing Execution Check-Lists

To access execution check-lists:

- Click the link of the e-mail sent to you.

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

  ☛ *(Option 2) In the **Hopex GRC** desktop, select **Assessment > My Activities > Check-lists To Complete***

Completing a Check-List

To complete the check-lists addressed to you:

1. See Accessing Execution Check-Lists.
2. Click the name of the check-list.
3. In the list that appears, answer the check-list questions.

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

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

Transferring a Check-List

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

To make a transfer request:

1. See Accessing Execution Check-Lists.
2. Click the name of the check-list.
3. Click **Submit** the **Request Transfer**.
   The manager is informed by e-mail and must reassign the questionnaire to another person.

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

MANAGING EXECUTION CHECK-LISTS

Accessing Check-Lists

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

To access check-lists:

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

Reassigning Check-Lists

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

☛ *For more details on how to transfer a check-list, see Transferring a Check-List.*

To reassign a check-list:

1. In the **Hopex GRC** desktop, select **Assessment > My Activities > Check-lists To Reassign**.
2. Select a check-list and open its properties.

CHECK-LIST RESULTS

To display the results of execution check-lists:

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

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

Results are displayed in columns:

- **Completion rate**: percentage of check-lists that are entirely completed (out of all check-lists)
- **Compliance rate**: number of "Pass" nodes / total number of nodes

  ☛ *Only questions of OK/KO/NA type are used for compliance rate computation.*

- The **Execution rate** is "Passed" if the compliance rate is greater than or equal to the compliance threshold.

  ☛ ***Sample size*** *and* ***Compliance threshold*** *are reminded for your information. Corresponding values were specified in the control properties.*

CONTROL EXECUTION REPORTS

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

See Control Execution Reports.

MANAGING COMPLIANCE

Hopex GRC enables control directors responsible for the implementation of compliance efforts to:

- import data from the UCF Common Controls Hub (Authority Documents, Citations and Common Controls)

  ☛ *To be able to use the import wizard, yo need to have **HOPEX UCF**.*

- define regulations with which the organization must comply, as well as its internal business policies
- define the perimeter of entities and processes subject to compliance
- assess IT compliance to applicable regulations

  ☛ *An specific assessment template is available. See Control Assessment by Entity and Regulatory Framework.*

- generate regulatory and IT compliance reports.

✓ About Unified Compliance Framework
✓ Managing the Regulatory Environment
✓ Managing the Compliance Register
✓ IT Regulatory Compliance Reports

About Unified Compliance Framework

UCF (Unified Compliance Framework) is the largest library of regulatory content available today. It contains:

- Authority Documents
- Citations
- UCF Controls

The Common Controls Hub lets you quickly retrieve the data you need from the underlying Unified Compliance Framework®.

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

Main UCF Concepts

Authority Documents

An Authority Document is a text that falls under any of following categories:

- regulations (rules of law that, if not followed, can result in penalties),
- guidelines,
- standards,
- best practices.

> ☛ *Authority Documents are converted to regulatory frameworks in **Hopex**. For more details, see Viewing Regulatory Frameworks.*

Citations

Citations are references extracted from the original Authority Documents. They are associated to UCF Controls.

> ☛ *Citations are converted to regulation articles or sections in **Hopex** (depending on whether the Citation is associated to a Mandated Control or not). For more details, see Viewing Regulation Articles.*
>
> - *Citation without any mandate, but containing other Citation becomes a regulation section.*
> - *Citation without any mandate and no children Citation become a regulation article that bears no relevance to the organization.*

UCF Controls

Common Controls are the specific steps or actions that must be met to fulfill a compliance mandate stated in a Citation.

> ☛ *They are converted to control directives in **Hopex**. For more details, see Viewing Control Directives.*

Depending on their relations with Citations, different types of UCF controls can be distinguished. For more details, see Links between UCF concepts.

Links between UCF concepts

Enforcement Level is determined by the association of the Common Control to a Citation within a given Authority Document and not by a specific attribute of the Common Control itself.

Citations are associated to UCF Controls, which can be:

- **mandated** (in **bold**)

  ☛ *Only Mandated Controls are mandatory.*

  Common Controls become mandated when they are applied to at least one Citation from any Authority Document.

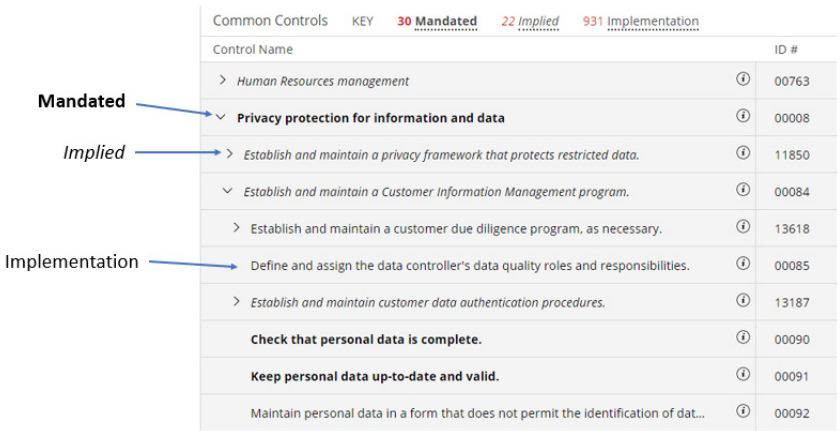
  A Common Control that becomes mandated has an impact on the Controls it supports and the Controls that, in turn, support it.

- *implied* (in *italics*)

  ☛ *Implied Controls are UCF Common Controls which are not mandated but contain Mandated Controls in their support structure.*

- Implementation

  ☛ *Controls supporting Controls become 'Implementation Controls'. They provide details not found in Mandated Controls regarding how to carry out the Mandated Control.*



Building a Shared List

A Shared List is a selection of Authority Documents that your organization needs to comply with and that you have chosen and saved in the Common Controls Hub workspace.

Lists can be created for documents related to geographic regions of your organization, specific subject matters ("Cybersecurity" or "Banking and Finance"). Select the Authority Documents you need to comply with. All associated Common Controls are automatically displayed in a harmonized, hierarchical list.

☛ *A Shared List becomes a control framework once imported to **Hopex** (a set of regulatory frameworks).*

Make sure your list only includes the Authority Documents you want to import into **Hopex**.

Mapping between UCF and Hopex Concepts

UCF	Hopex	Icon in HOPEX
Authority Document	Regulatory framework	
Citation Without Mandated Control Contains other Citations	Regulation section	
Citation Without Mandated Control	Regulation article	
Citation Without Mandated Control AND without Children	("leaf") Regulation article	
UCF Common Control	Control directive	

MANAGING THE REGULATORY ENVIRONMENT

You can:

- import UCF content from a Shared List built using the Common Controls Hub
- View the resulting regulatory frameworks and control directives in **Hopex**
- define what 'mandates' apply to the organization

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

To manage your regulatory environment in **Hopex**:

1. In the navigation bar, select **Compliance > Regulations**.

Using UCF Import

UCF Import Prerequisites

Internal Control directors and GRC Managers can upload UCF content (authority documents, citations and controls) and update it.

To be able to import this content to **HOPEX UCF**, you must have:

- **Hopex GRC** (or **Hopex Internal Control** as a minimum) AND **HOPEX UCF**
- a UCF account and API key
- a Shared List with the Authority Documents you want to import.

  > ☛ *For more information, see Unified Compliance Framework.*
- parameterized UCF options in **HOPEX UCF**

  > ☛ *In the UCF Common Controls Framework, information is generally available in English.*
  >
  > *If you want to use **HOPEX UCF** with **Hopex** user data language other than English, you must:*
  >
  > - *set up your data language of interest (example: if you want to use **Hopex** with French as data language, make sure to set up French as data).*
  > - *import UCF data*
  > - *repeat the operation (change data language + proceed to import) as many times as desired languages.*

Parameterizing UCF Import

To parameterize UCF import:

1. In the **Main menu**, select **Settings > Options**.
2. In the options window, expand **Tools > Data Exchange > Import > UCF Common Controls Hub Integration**.
3. Select the **Activate UCF Import** check box.

4. Enter the URL corresponding to UCF API.

   `https://api.unifiedcompliance.com/`

5. Enter your **UCF API Authentication Key**.

   ☛ *To retrieve your API authentication key in your Unified Compliance Framework workspace:*

   - *go to Settings > API Manager > API Keys.*
   - *Create Credentials and copy paste your API Key.*

6. Click **OK**.

Importing Data from the Common Controls Hub

Compliance officers need to set up the UCF environment in **HOPEX UCF**. This consists in:

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

To import UCF data:

1. In the navigation bar, select **Compliance > Regulations > Regulatory Frameworks**.
2. Click **Import UCF content**.
3. Click **Next**.
4. Select the Shared List from your Common Controls Hub.
5. Click **Next**.
6. Select the Authority Document(s) you wish to import into **Hopex**.

   ☛ *If you update an already imported Authority Document, it may be useful to compare the columns **Latest available UCF updates** and **Last imported UCF update**.*

7. Click **Next**.

Defining the Applicable Regulatory Content

Regulatory content relevance

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

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

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

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

Reviewing regulatory frameworks after UCF import

Once the UCF data has been imported, the following tree appears (available to manager profiles).

This tree displays:

- regulatory frameworks (Authority Documents)
- citations (Citations)
- associated control directives (Common Controls)

It is based on the supported/supporting structure originally defined by UCF.

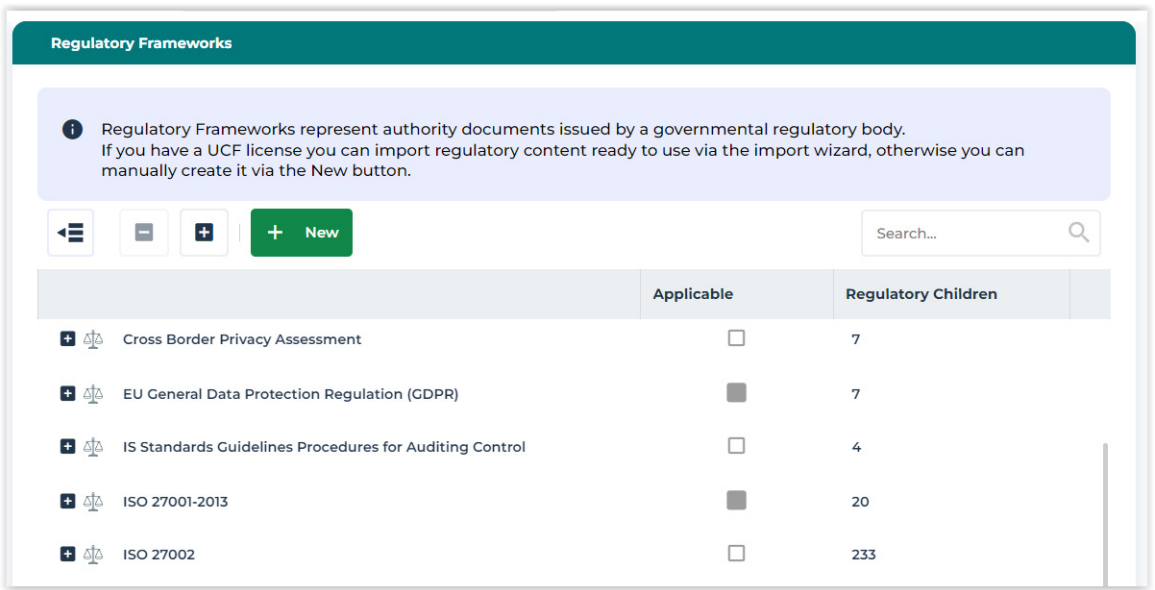
From this tree you can:

- review the newly imported regulatory frameworks and their content.
- specify the content applicable to your organization

Selecting relevant content for your organization

To declare regulatory content as relevant:

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



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

Data corresponding to the regulatory content you have selected become available to Internal Controllers in the Control Framework register. See Managing the Compliance Register.

MANAGING THE COMPLIANCE REGISTER

In the compliance register, internal controllers can manage:

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

  ☛ *If you have regulation frameworks and requirements in your repository and if you want to be able to reuse them in **Hopex GRC**, see Reusing Regulation Data.*

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

- rules that are internal to the organization: business policies

Concepts Used in the Compliance Register

HOPEX Concept	Definition
Regulatory framework	A regulatory framework is an authority document falling under any of following categories: regulations (rules of law that, if not followed, can result in penalties), guidelines, standards, best practices.
Article (of regulatory framework)	An article is a citation from a regulatory framework and is usually associated to a mandated control directive.
Section (of regulatory framework)	A section is a citation from a regulatory framework without any mandated control directive, but containing other sections or articles.
Control directive	Control directives are an interpretation of the law and contribute to the enforcement of any regulation article your organization has to comply with.
Policy framework	A policy framework consists of a number of business policies. Policy frameworks may contain sections.
Business policy	A business policy is an internal document issued by an organization (security measure, best practice, etc.).

Accessing the Elements of the Compliance Register

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

Displaying elements as a list

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

- without controls
- connected to controls which have never been executed
- connected to failed controls

To access these lists:

1. In the navigation bar, select **Compliance > Relevant Regulations**, then:
   - **Control Directives**
   - **Business Policies**

Columns indicate, for each control directive:

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

To list existing implementing controls or create one:

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

Displaying control directives in a tree of regulatory frameworks

To display control directives in a tree:

1. In the navigation bar, select **Compliance > Relevant Regulations > Control Objectives > By Regulatory Framework**.

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

- regulatory frameworks
- control directives implementing articles
- associated controls

Displaying business policies in a tree

To display business policies:

1. In the navigation bar, select **Compliance > Relevant Regulations > Business Policies > By Policy Framework**.

This tree enables you to view business policies your organization needs to comply with.

It displays:

- the number of implementing controls
- compliance rate

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

- the control level

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

Viewing Regulatory Frameworks

A regulatory framework falls under any of following categories:

- regulations (rules of law that, if not followed, can result in penalties)
- guidelines
- standards
- best practices

> ☛ *Regulatory frameworks correspond to UCF imported Authority Documents.*

Accessing regulatory frameworks

A regulatory framework tree displays relevant regulation articles.

To access the regulation framework tree:

- In the navigation bar, select **Compliance > Frameworks > Regulatory Frameworks**.

The tree starts from the regulatory frameworks and displays:

- the control directives enforcing the regulatory articles

  > ☛ *For more details on control directives, see Viewing Control Directives.*

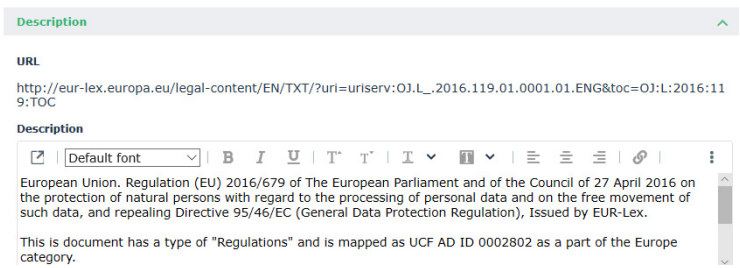
- **HOPEX** implementing controls, if any.

  > ☛ *For more details on controls, see Managing Controls.*

Regulatory framework overview & description

The **Overview** section of the regulatory framework characteristics enables you to display general characteristics originating from the Common Controls Hub.

> ☛ *These characteristics cannot be modified if the content comes from UCF.*



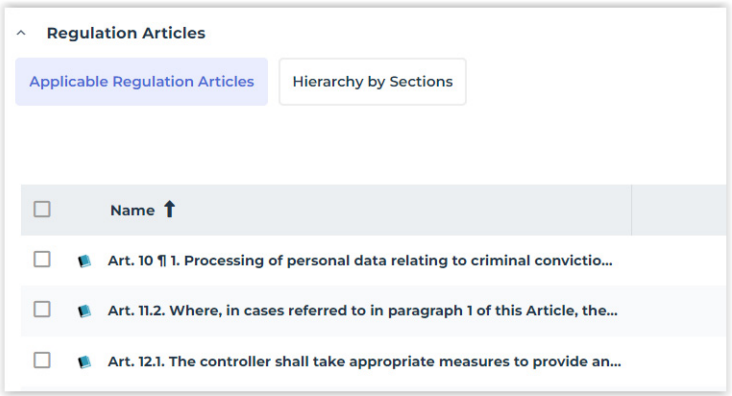
Content of a regulatory framework

To access the relevant regulatory content of a regulatory framework:

1. In the navigation bar, select **Compliance > Frameworks > Regulatory Frameworks**.
2. Select the appropriate regulation framework and open its properties.
3. Expand the **Regulation Articles** section.

From here you can access relevant regulations articles:

- through a list of **Applicable Regulation Articles**
- through a **Hierarchy of Sections**



Viewing Regulation Articles

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

> ☛ *Regulation articles correspond to the imported UCF Citations. For more details, see Main UCF Concepts.*
>
> ☛ *If the original UCF citation has children but is not associated to any UCF Common Control, it becomes a regulation section in **HOPEX UCF**.*
>
> *If the original UCF citation does not have children and is not associated to any UCF Common Control, it becomes a "leaf" (and irrelevant) regulation article.*

The property page of a regulatory article displays:

- the parent regulatory article or section
- children articles, if any
- the elements that are subjected to this regulatory article (entities or processes)
- the associated mandated directives

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

- implementing controls, if any

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

Accessing regulation articles

To access regulation articles:

1. In the navigation bar, select **Compliance > Frameworks > Regulatory Frameworks** and expand the tree.

Connecting or viewing objects subjected to a regulation article

It is possible to connect process categories/processes or entities to articles (or sections). It enables to specify which parts of the organization are subject to compliance.

To connect process categories/processes or entities to a regulation article:

- In the property page of the regulation article, expand the **Subjected Elements** section and connect objects as appropriate.

  ☛ *Once the entites, processes or process categories are connected to an article, an **Articles** tab appears in the scope of these objects.*

You can also view objects that are indirectly linked to the regulation article.

```
Example of indirect link: If a regulatory framework is
linked to an entity, the entity is indirectly linked to all
the regulation articles and sections of the regulatory
framework.
```

Enforcement of a regulatory article

To know more about the enforcement of a regulation article:

- Open the property pages of the regulation article and expand the **Enforcement** section.

You can view:

- Its associated **Control Directives**

  ☛ *You can view the qualification of the control directive in the corresponding column:*

  - *mandated*
  - *implied*
  - *implementation*

- its **Implementing Controls**

  Implementation controls that appear in this list are those connected to control directives of this section.

  ☛ *Internal controllers must design **Hopex** controls to implement directives. For more details on implementing controls in **Hopex**, see Managing Controls.*

Connecting Business Documents

You can link business documents to an article (or a section).

Viewing Control Directives

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

☛ *Control directives correspond to Common Controls imported from UCF. For more details, see Main UCF Concepts.*

Accessing control directives

To access the control directives of your register:

- In the navigation tree, select **Compliance > Relevant Regulations > Control Objectives > Control Objectives**.

  ☛ *First-level Implied control directives appear in this list only if one of their children is mandated.*

Some columns indicate:

- whether the control directive constrains the organization
- the number of implementing controls associated

From the drop-down list you can view the control directives sorted according to different criteria:

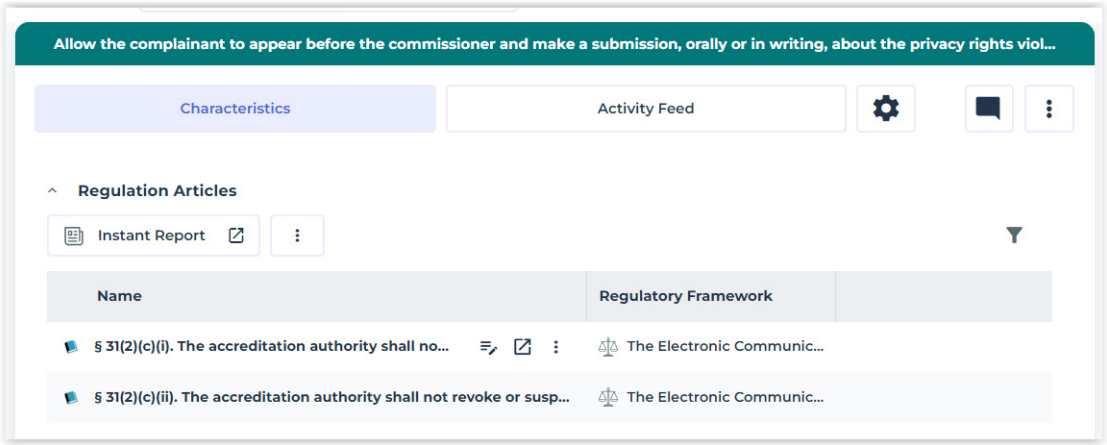
- **Control directives without controls**

  ☛ *To create a control on a control directive, expand the **Implementation** section.*
- **Control directives with controls never executed**
- **Control directives with deficient controls**

Viewing articles associated to a control directive

A mandated control directive is associated to a regulation article.

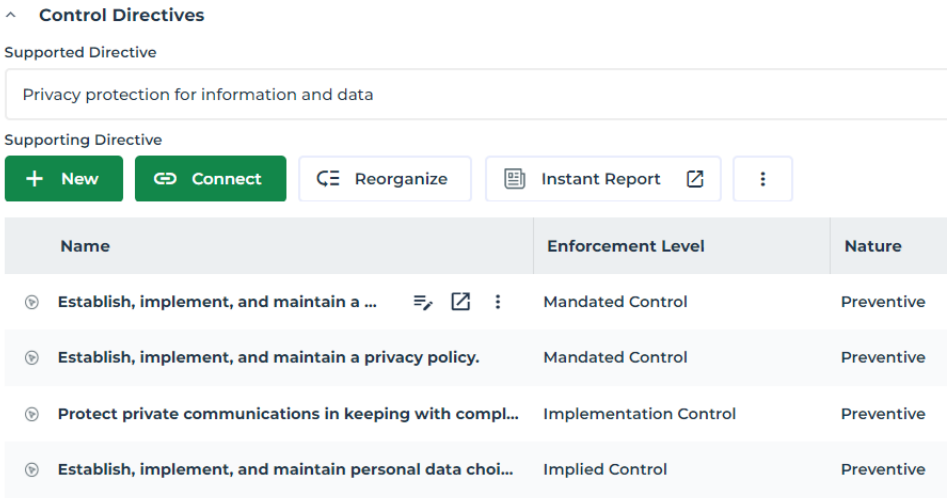
It is beneficial to have several regulation articles in the **Regulation Articles** section of a control directive. It means that your control directives enforce compliance of your organization to several regulation articles.



Supported and supporting directives

The properties of the control directive enable to view relations between control directives:

- Impacted control directive
- Contributing control directives



Enforcement level of control directives

There are three enforcement levels for each control directive:

- ***mandated***

  📖 *a mandated directive is directly associated to a regulation article. It implements a regulatory framework.*

- ***implied***

  📖 *An implied directive is a non-mandated control directive that is a parent of a mandated directive. It indicates that one of the control directives contained within its supporting hierarchy is mandated.*

- ***implementation***

  📖 *An implementation directive is a non-mandated directive that is a child of a mandated directive. It provides details regarding how to carry out the mandated directive and facilitates its implementation.*

Enforcement level for control directives	
Implied control directive	- Is not mandated - Contains at least a mandated control directive in its hierarchy - Allows to display the mandated control directives within the UCF hierarchy - Is supported by a mandated control directive
Implementation control directive	- Is not mandated - Appears under a mandated control directive (is supporting a mandated control directive)
Mandated control directive	- Is supporting an implied control directive - Can be supported by implementation control directives - Can support or be supported by other mandated directives

Viewing Hopex controls implementing a control directive

Columns in the list of control directives give you an overview of **Hopex** controls that are actually implementing each control directive.

To have a more detailed view of the controls on a control directive:

1. In the navigation bar, select **Compliance > Relevant Regulations > Control Directives**.
2. Open the properties of a control directive.
3. Expand the **Implementation** section.

   ☛ *You can also create controls from this section.*

You are given information on the control as well as on its execution results:

- **Control nature**

  ☛ *See Control nature.*

- **Control level**

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

  ☛ *See Control level.*

- **Latest compliance rate**
- **Latest execution result**

  ☛ *For more details on control contextualization see Executing Controls.*

Attaching business documents or external references

You may attach business documents to a control directive or create an external reference of URL type.

IT Regulatory Compliance Reports

Hopex GRC provides reports that enable to follow the IT and regulatory compliance process.

Reports enable to:

- view the compliance level of an entity with regulations.
  - ☛ *See Regulatory Compliance by Entity.*
- distinguish, for each regulatory framework, between control directives implemented by controls and control directives not implemented by any controls.
  - ☛ *See Control Directives Implementation by Regulatory Framework.*
- view compliance level for each regulatory framework.
  - ☛ *See Compliance by Regulatory Framework.*
- follow compliance process progress.
  - ☛ *See Regulatory Compliance Overview.*
  - ☛ *See Regulatory Compliance Progress.*
- view issues that impact a given control type (a control type related to IT compliance for example)
  - ☛ *See Issues by Impact.*

Regulatory Compliance by Entity

The "Regulatory Compliance by Entity" report displays the aggregated entity compliance level to applicable regulatory frameworks.

This report displays a tree of all the entity processes and applications for which a control connected to regulations has been assessed.

Access path

Navigation bar > Reports

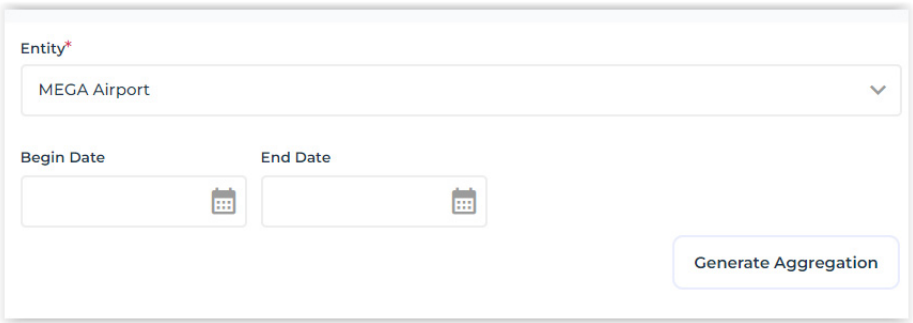
Parameters and Launch

To launch the report "Regulatory Compliance by Entity":

1. Enter the required parameters.

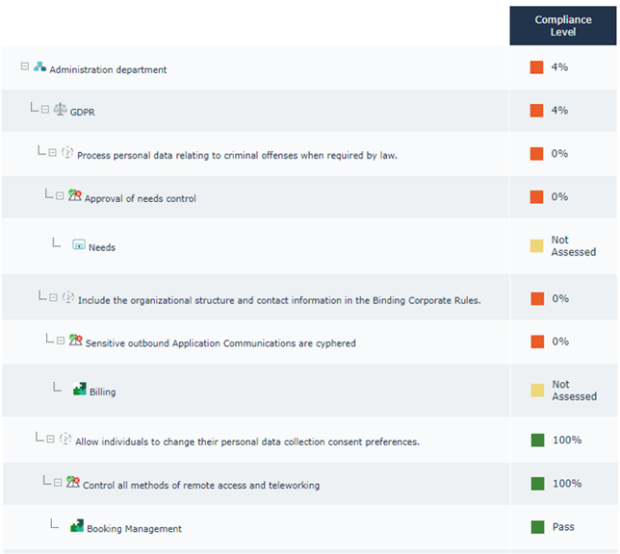
Parameters	Remarks
Entity	Mandatory Entity whose compliance level is to be computed.
Begin and end date	Optional Enables to define the time interval to take into account to aggregate assessment results. If no date is specified, all assessment data is taken into account for compliance level computation.

2. Click **Launch Aggregation**.



3. Click **OK**.

Example



Results for each object in this report are computed as follows:

Object type	Calculation
Application/Process (in the control scope)	Last control assessment in the context of the application or process. Possible results: - Pass - Fail - Not assessed
Control (implementing a control directive)	Percentage of pass controls (for context applications or processes) Note: here, Not assessed = Fail
Control directive (of a regulatory framework)	Average of control levels for controls connected to a control directive
Regulatory framework (with the root entity of the tree in its scope)	Average of control levels for control directives connected to the regulatory framework
Entity	Average of control levels for regulatory frameworks connected to the entity.

Control Directives Implementation by Regulatory Framework

This report enables the compliance officer to make sure control directives are appropriately implemented by controls.

It consists in a stacked bar chart, which shows the overall coverage of a given list of regulatory frameworks. A regulatory framework is considered as implemented if all the control directives are connected to a control.

Access path

Navigation bar > Reports

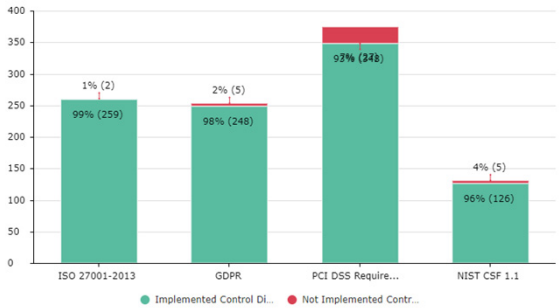
Parameters

Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frameworks.

Results

The report distinguishes, for each regulatory framework, the percentage of:

- control directives connected to at least one control (**implemented control directives**
- control directives not connected to any control (**Not implemented control directives**)



Compliance by Regulatory Framework

☛ *This report is also available in the form of widget to be added to your dashboard. To add it, from the navigation bar, click* ***Dashboard*** *then* ***Add a widget > GRC > Compliance****.*

It consists in a stacked bar chart, which shows the level of compliance with a list of regulatory frameworks.

Access path

Navigation bar > Reports

Parameters

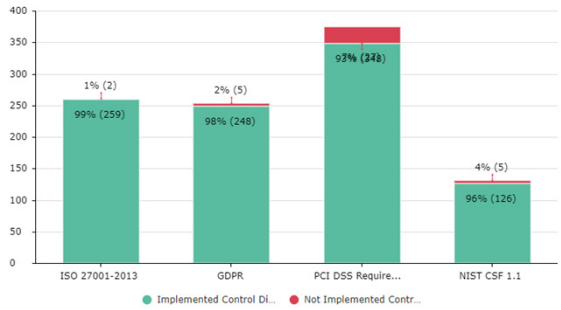
Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frameworks.

Results

Results are displayed in the form of bar charts.

Each bar displays the number of controls associated to control directives and enables to classify them as follows:

- **Pass**: controls whose Control Level = 100% (successfully passed the assessment)
- **Fail**: controls whose Control Level < 100% (did not obtain a satisfactory score)
- **Not assessed**: controls with no control level



Regulatory Compliance Overview

The "Regulatory Compliance Overview" report enables to follow-up the details of compliance to a specific regulatory framework.

Access path

Navigation bar > Reports

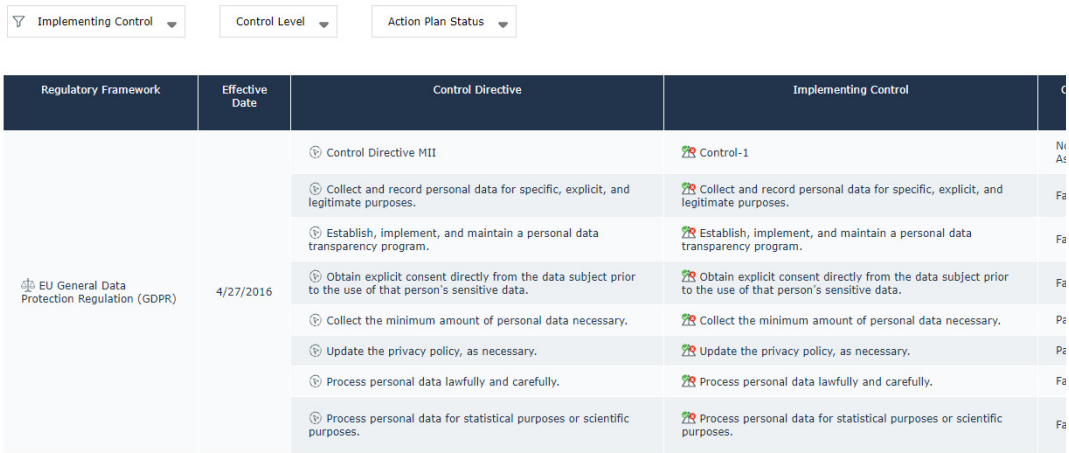
Parameters

Parameters	Remarks
List of regulatory frameworks	The report applies by default to all regulatory frame-works.

Results

From this report you can monitor, for each regulatory framework:

- ***Compliance %***: percentage of pass controls out of the number of controls connected to the regulatory framework control directives.
- ***Implementation %***: percentage of assessed controls out of the number of controls connected to the regulatory framework control directives.
- control assessments
  - ***Control level***
  - ***Last assessment control***
- issues and action plans implemented:
  - ***issue***
  - ***% of action plan progress***
  - ***action plan status*** (on time, delayed)
  - ***action plan cost*** (estimate of the action plan cost)



Regulatory Compliance Progress

This report is a radar chart showing the evolution over time of the compliance level of one entity with a given set of regulations.

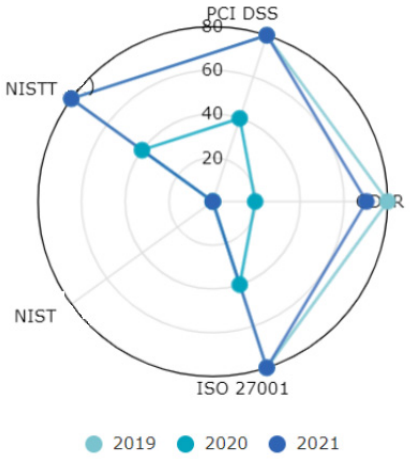
Access path

Navigation bar > Reports

Parameters

Parameters	Remarks
Entity	Organization whose compliance level is to be computed
Regulatory framework	Regulations to include in the chart
Calendars	Time periods taken into account to follow-up the evolution of the compliance level over time

Report example



CONTROL TESTING

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

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

The testing process consists of three phases:

- ✓ Preparing Control Testing
- ✓ Preparing Tests
- ✓ Executing Tests
- ✓ Test Follow-Up

PREPARING CONTROL TESTING

☛ *See also Contextualizing Controls.*

☛ *See also: GRC Functional Administration.*

Defining Test Sheet Questions

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

To create testing steps on a control:

1. In the control properties, select the **Testing** page.
2. In the **Test Steps** section, click **Create a Questionnaire**.
3. In the dialog box that appears, drag & drop an "OK/KO" question.
4. Click **Save and Close**.

Defining Testing Methods

☛ *To be able to define the testing method, you need to have created questions (testing steps) on controls.*

To specify control test characteristics:

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

☛ *For more details, see Specifying or modifying the sample size.*

PREPARING TESTS

Functionalities described here essentially concern the GRC manager.

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

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

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

Creating Test Plans

The test plan is prepared by the internal control director.

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

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

To create a plan:

1. In the navigation bar, select **Testing > Test Plans**.
2. Click the **New** button.
   The new plan appears.
3. Open the properties of the plan.
4. In the **Characteristics** tab, modify the **Name** of the plan.
5. Select the **Nature** of the plan:
   - Audit
   - Test
   - Compliance
   - Mixed

   > ☛ *If you only have **Hopex Internal Control**, the plan nature is automatically specified and cannot be modified.*
   >
   > ☛ *Depending on the selected nature, a **Tests** and/or **Audits** tab appears in the properties of the plan.*
   >
   > ☛ *If you selected "Test" or "Mixed" values, an assessment campaign is created at validation of the plan. This will enable generation of questionnaires to internal controllers for assessment of controls. For more details, see Assessing Controls.*
6. Select the **Calendar** of the plan.
7. Modify the **Begin Date** and the **End Date** if necessary.

   > ☛ *The **Status** is defined automatically by the workflow.*
8. Click **Save**.

The plan is created.

You can now create tests directly in the plan page.

Planning Tests

Test planning is carried out by the GRC Manager.

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

Creating a test

To create a test:

1. Click **Test > Test Plans**.
2. Open the properties of the plan that will include the test to be created.
3. Select the **Tests** page.
4. Click **New**.
   The new test appears under the plan.

☛ *To define characteristics of the test, see Defining test properties.*

Accessing tests

To access tests of a test plan:

❱ Click **Test > Test Plans** and expand a plan.
The tests (or audits, depending on the plan nature selected) corresponding to the plan appear.

Defining test properties

You can specify certain information on tests.

See also Viewing a test dashboard.

General characteristics

General characteristics of the test are:

- **Name**: test name.
- **Code**: you can assign a code to the test.
- **Included in the Initial Plan**: this attribute is defined automatically according to plan status at the time of creation of the test. It indicates if the test was present at plan creation, or if it was added later.
- **Entity** controlled
- **Lead Controller**: lead controller name.
- **Main Control Correspondent**
- **Objective** of the test.
- **Category** of the test:
  - "Compliance"
  - "Efficiency"
- **Status** of the test: this attribute is defined automatically and modified at workflow transitions.

Justification and workload

In this section you can enter the following characteristics:

- **Origin**: follow-up, specific, recurrent, etc.
- **Priority**: priorities can be specified for tests. You can select tests to be integrated in the plan based on this priority criterion.
- **Estimated Duration** (days).
- **Estimated Resources**
- **Estimated Workload**

  ☛ *The following characteristics are automatically calculated:*

  - ***Effective Workload (Hours)**: calculated from the effective workload defined on time sheets or on activities if no time sheet has been entered.*
  - ***Estimated Number of Resources***
- **Justification** of the test

Scope

In this section you can connect process categories or processes to the test.

These can be used to automatically generate the test work program.

☛ *For more details, see Completing the work program manually.*

Milestones

In this section, you can indicate a **Planned Begin Date** and a **Planned End Date**. These dates constitute audit milestones.

☛ *You can choose to enter milestones at a later stage.*

Users

In this section you can specify the stakeholders of a test:

- **Test Controller**: controllers having been previously defined, you can connect but not create controllers. See Assigning resources to tests.
- **Person tested**
- **Other Participant in Test** (for information only)

Skills

In this section you can specify the skills required by controllers to execute tests.

To define skills required for the test:

1. In the **Skills** frame, click **New** or **Connect** to create a skill or connect an existing skill.

When assigning controllers to a test, you will be able to compare skills of controllers with skills required for the test. For more details on the report providing this information, see Assigning resources to tests.

Summary

In the **Conclusion** section, you can specify:

- **Key Strengths**
- **Key Weaknesses**
- **Evaluation**: good overall level, can be improved, etc.

> ☛ *The value specified here is displayed in the test dashboard, at the top of the **Characteristics** page.*

Test Activities

A specific page in the properties of the test enables to view test activities.

Deficiencies

A specific page in the properties of the test enables to view deficiencies.

Viewing a test dashboard

To access a test dashboard:

1. See Accessing tests.
2. Open the properties of a test.

The **Characteristics** page displays a dashboard containing essential information about the test:

- **Progress** % = number of test activities in "closed" status / number of activities in the test
- **Evaluation** of the test:
  - Good overall level
  - Can be improved
  - etc.

> ☛ *This evaluation is performed by the audit director.*

- **Issues**: displays the number of issues

Creating "template" tests

"Template" tests are work programs specially prepared to be applied to new tests.

This status is exclusively reserved for tests of a plan which is itself defined as a template. It applies automatically to existing tests of the template plan, and is proposed at creation of a new test on this same plan.

To define a test plan as a template:

1. Click **Test > Test Plans**.
   The list of plans appears.
2. Click the icon of the plan in question and select **To Be Validated > Set As Template**.

Selecting tests to be executed

Viewing the test coverage report

Hopex GRC supplies a report providing information on the number of tests executed on each entity between two dates. It indicates entities that require testing, and enables generation of the corresponding tests.

To access this report:

1. Click **Test > Preparation > Entity Coverage**.
2. In the edit window, select a begin date and end date.
3. (Optional) select the score obtained by the test or its status.

For each tested entity the report presents:

- the **Number of tests** executed between the two dates (effective begin and end dates)
- the **End date** of the last test (effective end date), or its state if it is still in progress
- the name of the **Last Test**.
- the **Score** of the last test.

To generate tests corresponding to one or several entities:

- Select the entity or entities that interest you and click the **Generate Tests** button.
  A wizard asks you to choose a target plan. The tests are generated.

Viewing previous audit expenses

A report allows you to view expenses of previous missions.

To access this report:

1. Click **Test > Test Plans**.
2. Select a plan and in its properties select the **Reports** page.
3. In the drop-down list, select **Expenses**

You can view expenses:

- By category
- By resource (auditor, controller or tester)

Selecting tests to be integrated in the test plan

Tests become active after validation only. Among all tests, some are part of the definitive plan, while others are discarded.

Hopex GRC proposes tools simplifying selection of tests to be integrated in the plan.

Discarding tests

Potential tests considered of low priority can be discarded via the workflow.

To discard a test:

- Click the icon of the test to be discarded and select **To Be Validated > Discard**.

The test is discarded but not deleted. It could serve as a template for a new test the following year.

Validating tests

You can validate tests:

- globally, at validation of the test plan
- individually

Planning tests using a Gantt chart

A report allows the internal control director (or GRC manager) to plan the different tests of a test plan.

To display this report:

1. Under **Test** > **Test Plans**, select the plan properties.
2. Select the **Schedule** page.
   A Gantt chart describes tests of the plan.

The schedule shows data of the current year. You can view tests within the framework of a more specific time period.

To define the display period in the Gantt chart:

- select a calendar period, or
- specific begin and end dates.

To modify dates for an test in the chart:

- Click the center of the period and move the mouse to simultaneously move the begin and end dates.

Assigning resources to tests

Before assigning a resource to a test, you can view its availability and skills.

Viewing resource availability

To view resources available with necessary skills for a test:

1. Open the properties of the test plan concerned.
2. Select the **Assign Resources** page.

   ☛ *By default, the report presents tests of the test plan over the year. You can display those of a particular period.*
3. In the table at top left, select a test.
4. In the table at top right, select a resource of which you wish to display availability.

   ☛ *You can select several resources.*
5. In the lower frame, click the **Refresh** button.

Two charts present:

- Skills required by the test and skills of the selected resource.
- Availability of the resource on test dates.
  The color of the test period depends on the number of resources assigned to it related to the estimated number of resources:
  - Green if the test has a sufficient number of resources
  - Yellow if resources are insufficient
  - Red if no resources are assigned

    ☛ *These two charts should be refreshed separately.*

Assigning a resource to a test

To assign a resource to a test:

1. In the **Assign Resources** page of the test plan properties, in the top left frame, select the required test.
2. In the top right frame, select a person and select the **Assign** check box.

   ☛ *To remove an assignment, perform the same procedure and clear the **Assign** check box.*

Specifying a lead controller for a given test

To specify the lead controller on a test:

1. Open the properties of the test concerned.
2. Specify the **Lead Controller** field.

Sending the Notification Letter

After having completed the specifications required for execution of a test, the internal control director can send a notification letter informing controlled persons of the test.

Sending this notification letter is not included in the workflow. It precedes the step in the workflow that consists in publishing the test.

Creating notification letters

To create the test notification letter:

❱ Click the icon of the test and select **Deliverables > Notification Letter**. A message asks if you want to open or save the file. The document presents the comment entered in characteristics of the test.

When the document has been saved, you can open and modify it.

You can also connect it to the test as a business document, under the "notification letters" category. For more information, see Using Business Documents.

Connecting the notification letter to the test

The file is generated from test content, but is not connected by default to the test.

To connect the notification letter to the test:

1. Open properties of the test.
2. Select the **Documents** page and the **Business Documents** tab.

3. Drag and drop the notification letter that was previously generated. The document appears in the list of documents attached to the test.
4. Open the document properties and in the **Document Pattern** field, select "Notification Letter".

☛ *For more information, see Using Business Documents.*

Validating tests

When the internal control director decides that a test should be executed as part of the test plan, he/she validates the test.

☛ *An assessment session is created. This will enable generation of questionnaires to internal controllers for assessment of controls. For more details, see Assessing Controls.*

Publishing tests

Hopex GRC enables preparation of tests and only making these public to controllers when planning is completed.

To make a test public:

1. Right-click the icon of the test.
2. Select **To Be Published** > **Publish**.

Test status changes to "Published".

Having been published, tests appear in the work program of controllers.

Preparing Tests

Supervision of test progress is assured by the lead controller. In the test preparation phase, he/she establishes the work program and assigns activities to controllers.

Work program creation prerequisites

So that the work program can be generated:

- process categories or processes must be connected to the entity
- controls must be connected to process categories/processes

Work program content

Hopex GRC enables automatic creation of a work program structure from:

- the tree of processes connected to the entity, or
- the processes specified in the test scope

☛ *If no process has been specified in the test scope, all processes connected to the entity will appear in the work program.*

Environment objects	Objects created in the work program
Process category or process	Test theme
Control (connected to the process category or process)	Test activity

☛ *The entity is represented by the test.*

Test theme

A theme corresponds to a process category or a process.

Themes can be used to group test activities and workpapers, that is to organize test content.

Test activity

A test activity corresponds to a control.

It is the basic element of the test. It enables assignment of responsibility to the controller.

Workpaper

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

A workpaper is generated for each generated test activity. For more details, see Creating workpapers.

Accessing the tests to prepare

To access the tests you need to prepare:

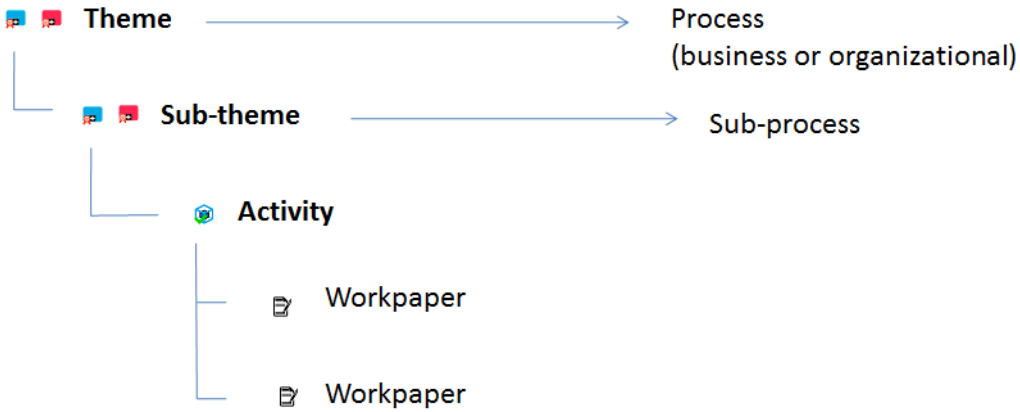
❱ In the navigation menu, click **Testing > Execution > Global**.

Creating work programs automatically

To create a work program automatically:

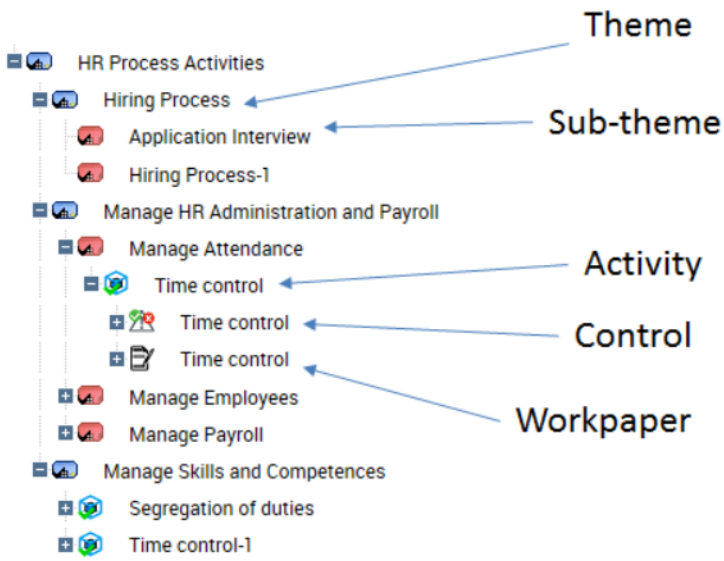
1. See Accessing the tests to prepare.
2. Click the test icon and select **Generate Work Program**.
   This is going to duplicate the process category/process tree for the entity within the test scope.

If processes are explicitly specified in the test scope, only these processes are automatically generated in the work program structure.



Completing the work program manually

The lead controller can complete the test manually to specify its content. He/she can add or remove themes/activities in the **Work Program** page the test.



Creating themes

To create a theme:

1. In the **Work Program** page of a test properties, click the icon of a pre-generated test theme and select **New > Test Theme**.

2. Display properties of the theme.
   You may:
   - select a parent test theme (if you want to create a tree of themes)
   - connect the test theme to a process (test theme scope)
   - enter a comment

You can view the tree of themes and sub-themes created. You can now create activities and workpapers.

Creating activities

A test activity is a test element relating to a control.

To create an activity:

1. In the **Work Program** page of a test properties, click the icon of a theme and select **New > Test Activity**.
2. Display properties of the activity.
3. Connect the test activity to a control.
4. Select the **Owner** of the test activity, who can be a controller or the lead controller of the current test.
5. Indicate the **Estimated Workload**.

   ☛ *You can later manually enter the effective workload on this activity.*

Assigning activities

Assigning an activity

For each activity, the lead controller specifies:

- Start and end dates
- Estimated workload
- Controller responsible for execution

To enter this data:

1. In the properties of the test, select the **Activities** page.
2. Open the properties of the test activity concerned.
3. In the **Owner** field, using the right-pointing arrow, select a controller from among the candidate controllers.
4. Enter test activity start and end dates.
5. Specify the workload.

Assigning multiple activities to the same controller

To assign multiple activities to the same controller:

1. In the properties of the test, select the **Activities** page.
2. Select your activities and click the **Assignment** button.
3. In the multiple assignment wizard, select the **Test Activity Owner**.
4. Click **OK**.

Reviewing the Work Program

The lead auditor can proceed with a report on the work program. This report allows to check that:

- task assignment has been correctly carried out
- the work program covers the appropriate risks and processes

Consulting the work program report

To access work program reports:

- In the page of a test, select **Reports** > **Work Program**.

You can view:

- comparison of resources allocated and resources available
- workload (in person/days)
- workload by theme (in person/days)
- activities by theme

Exporting the workload under Excel

The work program under Excel covers themes, sub-themes, activities and workpapers.

Having the work program available under Excel allows:

- consultation of the complete work program without having to access objects individually
- storage of a printed version of the work program
- viewing tasks to be executed at indication of an issue

To export the work program:

- In the **Work program** page of the test, click the tree root and select **Deliverables > Export Work Program (Excel)**.

  ☛ *A pop-up window opens at the bottom of the page. If your navigator blocks these windows, you cannot see file export. In this case, deactivate pop-up blocking in the navigator.*

You can modify the work program in Excel.

When the work program has been modified, you must create a business document in **Hopex GRC** and re-import the modified work program.

To create the business document corresponding to the modified work program:

1. In the properties of the test, select the **Documents** page.
2. Select the **Business Document** tab and drag-and-drop the work program Excel document.
   The modified work program is now stored in the **Hopex** repository.

   ☛ *In the properties of the business document, you can specify "Work Program" as a **Document pattern**.*

Validating work programs

When the lead controller validates the work program via the workflow, an assessment session is automatically created and connected to the test. Assessment

questionnaires are generated and made available from test activities. Respondents are owners of test activities.

☛ *For more details, see Assessing Controls.*

To validate the work program:

- Click the icon of the test and select **To Be Validated** > **Validate**.

Executing administrative tasks

Planning resources

Controllers can be assigned different tests at the same time. It is therefore important to enter the time allocated for each auditor to a test.

To indicate for each controller the time to be allocated to a test:

1. In the properties of the test, expand the **Responsibilities** section.
2. Select the **Controller in test** tab.
3. Select a user and in the **Workload (Hours)**, enter the time to be spent on the audit/test.

Creating general tasks

For controllers, the director can create tasks not directly linked to tests.

To create a general task:

1. Select **Testing > Preparation > General Tasks**.
2. Specify dates and a comment and connect users to this task.
   Users assigned to this task can allocate hours to this task in their time sheet.

Validating Vacations

To display vacations in auditor time sheets, you must previously have validated the vacation.

To validate the vacation:

1. Select **Test > Preparation > Vacation Requests** and open the properties of the vacation to be validated.
2. Position its status as "Validated".

Initializing expense sheets

The lead auditor can create an expense sheet per auditor/controller for all auditors/ controllers assigned to the audit/test. In this case it consists of initializing expense sheets.

To initialize expense sheets:

1. In the audit/test properties window, select the **Expenses** page.
2. Click the **Initialize** button.
   An expense sheet is created for each auditor/controller.

To create an expense:

1. In the expense sheet properties, expand the **Expenses** section and click **New**.

2. Enter for each expense:
   - an **Amount**
   - a **Date**
   - the **Expense Category**: "Lodging", "Food and Beverages", "Transportation"
   - a **Comment** if required.

     ☛ *The auditor enters the amount in the desired currency. The converted amount is calculated automatically.*

EXECUTING TESTS

☛ *Procedures described here apply to the "Internal Controller" profile only.*

Preparation of a test work program allows internal controllers to:

- execute tests on samples using test sheets.

  ☛ *These test sheets are presented in the form of check-lists. Questions are asked for each object present in the constituted sample.*

- assess controls in terms of design and efficiency by means of questionnaires.

  ☛ *These are the same questionnaires as those covered in the chapter concerning assessment campaigns.*

Consulting the Work Program

The internal controller needs to consult his/her work program.

To access tasks to perform:

❱ In the navigation bar, click **Testing > Execution > My Activities**.

Executing Tests on Samples

Internal controllers execute the test steps defined on controls on samples.

To be able to complete test sheets, you must first:

- generate or create workpapers
- specify or modify test sample size
- generate the test sample
- define test sheet questions

Creating workpapers

Workpapers are folders or work documents that serve as a basis for the controller in execution of the test.

☛ *Workpapers are created automatically at generation of the work program. For more details, see Work program content.*

To create a workpaper manually:

1. In the properties of a test, select the **Work Program** tab.
2. Select the activity concerned and display its properties.
3. In the **Characteristics** page of the activity, **Workpapers** section, click the **New** button.
   The workpaper appears:
   - in the test activity page
   - in the tree of the test work program

4. In the work program, select the paper to display its **Properties**.
5. Enter a name and your comments.
6. Click **OK**.

Specifying or modifying the sample size

The controller must specify the size of the test sample on the workpaper. This is the number of elements to be tested.

To specify sample size:

1. In the properties of a test, select the **Work Program** page.
2. From the work program, open the properties of a workpaper.
3. Specify the **Sample Size**.
   This is the size of the sample selected for testing.

   ☛ *By default, the value is inherited from the sample size specified on the control. For more details, see Defining Test Sheet Questions.*

Generating the test sample

Test samples are generated directly from information available on the control (test steps).

To generate samples:

1. In the properties of a test, select the **Work Program** page.
2. From the work program tree, click the icon of a workpaper and select **Generate Test Sample**.
   Depending on the previously specified sample size, a message informs you of the number of elements that will be created in the test sample.
   Generated test samples are available in the properties of the workpaper

Defining test sheet questions

Workpapers contain test sheets, which represent in tabular form the points to be executed. These test sheets contain:

- in rows, the elements of the sample to be controlled
- in columns, the questions (represented by test steps)

You must define check-list questions before being able to generate test sheets.

☛ *For more details, see Preparing Control Testing.*

Completing the generated test sheets

To be able to view test sheets, you must first:

- define test sheet questions

  ☛ *See Defining Test Sheet Questions.*
- generate the test sample

  ☛ *See Generating the test sample.*

To view the test sheet:

1. In the properties of a test, select the **Work Program** page.
2. Open the properties the question that interests you.

3. Select the **Test Sheet** tab.
   This test sheet presents:
   - in rows, the elements of the test sheet to be controlled
   - in columns, the test steps

You can reply to the questions in the columns provided.

Assessing test activities

Having specified test sheets, the controller can globally assess the test activity.

☛ *This "expert view" assessment can be based on results of test sheets, or not.*

To assess the test activity:

1. Open the properties of the test activity.
2. In the **Test Result** field, specify if the test has:
   - Failed
   - Passed
   - Not yet been assessed

Assessing Controls

Internal controllers must assess controls in terms of design and efficiency.

☛ *This assessment uses standard assessment campaign mechanics. Generated questionnaires are distinguished from those corresponding to test sheets.*

Generating questionnaires

The questionnaires are generated at validation of the work program.

☛ *For more details, see Validating work programs.*

Responding to Questionnaires

You can answer control assessment questionnaires:

- on a test
- on each activity of a test

To view test questionnaires:

1. In the navigation bar, select **Testing > Test Plans**.
2. In the properties of the test, expand the **Assessment** section.
3. Select a questionnaire and click **Display Questionnaires**.
4. Select the questions and reply to these in the lower part of the window.
5. Click **Save**.

To view test activity questionnaires:

1. In the properties of a test, select the **Work Program** page.
2. In the pop-up menu of a test activity, select **Assessment**.

Managing Time and Expenses

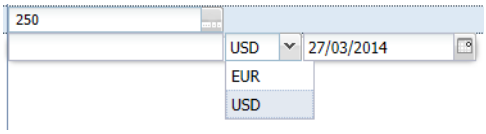
Managing Expenses

Auditors/controllers assigned to an audit/test can create expense sheets on this audit /test. In this case, they must submit their expense sheet to the lead auditor via a workflow.

To create an expense sheet:

1. In the navigation bar, select **Testing > Time & Expenses > Expenses**.
2. Click **New**.
3. In the **Expense Owner** field, select the audit/test concerned.

   ☛ *You can also create an expense sheet in the **Expenses** page of the audit/test properties. In this case, you do not need to specify the expense owner.*
4. Click **OK**.
   An expense sheet is created. You can now create associated expenses.
5. In the **Expenses** section of the expense sheet, click **New**.
6. In the properties of the expense sheet, enter an **Amount** and a **Date**: you can enter the amount in the currency you require (from those you can access).



   ☛ *The amount is converted to the currency configured for your user.*
7. Specify if required:
   - the **Expense Category**: "Lodging", "Food and Beverages", "Transportation"
   - a **Comment**.
8. Click the icon of the expense sheet and submit it via the workflow.

   ☛ *The lead auditor does not need to seek approval for his/her expense sheets.*

   ☛ *You can export to Excel the data contained in expense sheets.*

Entering Vacations

Entering vacations enables to:

- improved planning of test campaigns.
- pre-filling time sheets.

To enter a vacation:

1. In the navigation bar, select **Testing > Time & Expenses > Vacation Requests**.
2. Click **New**.
3. In the properties, select the associated **Plan**.

4. Also specify:
   - **Vacation Type** (holiday, training, other)
   - planned and effective begin and end dates
   - a comment if required
5. In the **Status** field, select "Submitted".

> ☛ *So that the vacation will appear in the time sheet, the lead controller must have validated the vacation (by positioning its status value on "Validated").*
>
> ☛ *An auditor/controller can modify or delete a vacation as long as the vacation has not been validated.*

Completing a Time Sheet

Auditors/controllers can complete time sheets in the framework of their audit/test.

To complete a time sheet:

1. In navigation bar, select **Testing > Time & Expenses >Timesheets**. The time sheet displays one line per audit.
2. Enter for each day the number of hours spent on each audit.
3. Click **Submit** to save your time sheet.
4. Click **Next** to enter your hours concerning the next week.

> ☛ *Messages may appear if the activity report is not consistent. For example, if hours have been allocated to an audit/test and the audit/test has not yet started. You can however submit an incomplete time sheet.*

The time sheet enables entry for each day and for each week the number of hours spent on each audit/test.

> ☛ *Only those audits/tests that have been published are visible in the time sheet.*

The time sheet also shows:

- vacations that have been validated
- general tasks (meetings, training, team management, administration ...)

Management of issues and action plans

The controller completes the work program by entering:

- Issues
- Action Plans

Managing Issues

Creating Issues

To create an issue:

1. In the navigation bar, select **Testing > Remediation > Issues**.
2. Click **New**.

In the properties of an issue you can qualify its **Impact**.

> ☛ *Issues can also be found in the work program and in the test activity properties.*

Saving test evidence

You can connect business documents or specify an URL address to illustrate an issue.

To add a document as an attachment:

1. In the tree of the work program of a test, select an issue to which you wish to add a document.
2. Expand the **Attachments** section.
3. In the **Business Document** drag-and-drop a document.

   > 🕮 *A business document is a document whose content is independent of the repository. This document can be MS Word, MS Powerpoint, or other files. A report (MS Word) generated on an object can become a business document.*

   The document appears in the list of documents attached to the issue. It is owned by the test of the issue. You can therefore also see it appear in the **Documents** tab of the test.

Managing Action Plans

Action plans can be created from issues.

To create an action plan:

- In the property page of an issue, expand the **Action Plans** page and click **New**.
  The action plan appears in the section.

Supervising Tests

The lead controller must validate the work of controllers via the activity workflow.

He/she can then check their work and assure test follow-up. To simplify the task, reports enabling test check are available on each test.

Test check reports

To access test check reports:

- In the properties of a test, select the **Reports > Supervision** page.

Three reports appear:

- **Issue Objectivity**: to ensure objectivity of issues, evidence must be provided.
  The figure displayed represents the percentage of issues with at least one attachment.
- **Work progression by controller**
- Controller activity **Summary Table**

Time Sheet Follow-up Reports

Reports enable follow-up of auditor/controller time sheets.

☛ *These reports are available for Compliance Managers only.*

To access the Reports tab:

❱ In navigation bar, select **Testing > Time & Expenses >Timesheet Follow-up**.

Test expenses reports

To view expenses of an audit/test:

❱ In the properties of a test, select the **Reports > Work Mission Expenses** page.

Pie diagrams present breakdown of expenses:

- by resource (auditor)
- by category:
  - Food and Beverages
  - Lodging
  - Transportation

To view the list of expenses associated with a diagram sector:

❱ Right-click in a sector.
Corresponding results appear as a list in the lower part of the window.

Concluding Tests

Test assessment reports

Reports allow the lead controller to best assess the test and analyze its action plans.

To access the Reports tab:

❱ In the properties of a test, select the **Reports > Assessment** page.

Several reports are proposed:

- Controls (Failed, Passed, Not evaluated)
- Action plan breakdown by priority (low, medium, high)
- Summary table of above elements
- Issues by theme

Generating test reports

The test report uses test elements.

To generate the test report:

1. In the properties of a test, select the **Work Program** page.
2. Click the icon of the test and select **Deliverables > Test Report**.
   A message asks if you want to open or save the file.
3. Save the file to be able to modify and then submit it.

Assessing tests

To assess the test:

1. In the **Characteristics** page of the test properties, select the **Summary** section.
2. You can indicate:
   - Test **Key Strengths**
   - Test **Key Weaknesses**
3. In the **Assessment** field, specify a value from:
   - "Good overall level"
   - "Can be improved"
   - "Improvement needed"
   - "At risk"

Terminating tests

When the test is closed:

- the test report is sent to persons interviewed
- action plans are sent to their owner

Closing tests

When the test has been terminated, the internal control director can close it.

☛ *Closing a test closes all objects at a lower level, with the exception of action plans and actions. When these objects have been closed you can no longer modify them.*

☛ *The administrator can exceptionally reopen these objects if necessary.*

TEST FOLLOW-UP

Implementing Action Plans

Listing action plans

To list your action plans:

- In the navigation bar, select **Action Plans > Action Plans > Action Plans to Implement**.
  This list presents the action plans assigned to you.

Implementing actions

The action plan owner must create actions.

Creating actions

To create an action:

1. Open the properties of a test.
2. In the **Action Plans** page, select an action plan to open its properties.
3. In the **Actions** section, click **New**.
4. Open the properties of the action created.
5. Modify its name if necessary, enter a date limit and an action owner.
6. Click **OK**.

Sending or submitting the action plan

Actions created and assigned to appropriate users constitute an action plan.

To submit the action plan:

- Right-click the action plan name and select **To Be Sent** > **Send**.

The approver validates the action plan by return.

☛ *By default, the approver is the controller who created the action plan.*

Action plan implementation follow-up

When the action plan has been validated by the approver, actions are implemented by persons concerned.

Specifying action plan progress

The action plan owner must inform the approver on progress of his/her actions.

To indicate progress of an action plan:

1. In the properties of an action plan, expand the **Progress Update** section.

2. Click the **New** button.
   A progress state is created.
3. In the **Progress Update Percentage** field, specify an action plan execution percentage.
4. Enter a comment if required.
5. Click **OK**.

☛ *Several progress states at different dates can be created.*

Following up action plan progress

After a predetermined period, the internal control director or lead controller can request receipt of information on progress of action plans.

To follow up action plan progress:

❱ In the action plan properties, select the **Progress Report** page.

Test Plan Follow-Up

Hopex GRC enables follow-up of test plans according to different criteria.

Displaying test plan follow-up reports

Reports enable test plan execution follow-up.

To access test plan reports:

1. Open the properties of the plan.
2. Select the **Plan Reports** page.

Supervision

This report offers a summary of test plan tests according to different criteria:

- Origin
- Priority
- Category
- Score
- Status

Workload and resources

This report enables comparison of estimated and effective workloads.

Pie charts show comparison of test design and efficiency.

Resources allocation

The diagram displayed in this report enables comparison of:

- persons available
- persons required
- persons assigned

By default, results relate to the current year, but you can display results for a precise period.

Gantt report

The Gantt report comprises two parts:

- A Gantt chart of plan tests scheduled between selected dates
- A Gantt chart of occupation of controllers on plan tests between selected dates

Expenses

This report shows all expenses linked to a plan, as well as breakdown by expense category and by controller.

It allows the director to plan future audits.

Closing a test plan

When all test activities have been completed, the internal control director can close the test plan.

The effect of this action is to close all tests in progress that have not been canceled.

Testing Dashboard

Your dashboard allows you to access a set of widgets and follow the progress of your tests in real time.

To customize your dashboard:

1. In the navigation bar, select **Dashboard**.
2. Click **Add**.
   The list of elements you can display in your dashboard appears:
   - general widgets
   - GRC-related widgets
3. Select an element.
   It appears in your dashboard.

MANAGING ISSUES AND ACTION PLANS

Issues are identified from control assessment questionnaires. Their analysis enables implementation of the appropriate corrective actions in the form of action plans. Action plan follow-up is simplified by production of reports.

MANAGING ISSUES

Creating Issues

You can create issues at all times, for example when a test activity was poorly evaluated.

To create an issue:

1. In the navigation bar, Select **Testing > Remediation > Issues**.
2. Click **New**.
3. Enter a **Name.**
4. In the **Category** field, specify whether the issue:
   - was detected at control assessment
   - was detected when performing tests
   - is generic
5. Specify the **Impact**: enables to qualify the impact of the issue (low, high..)
6. Enter a **Description**.
7. Click **OK**.

Scoping an Issue

You can specify how the issue has been detected.

To define the scope of an issue:

1. In the properties of the issue, expand the **Assessment Scope** section.
2. Connect:
   - a test activity, or
   - one or several assessed controls

Remediating Issues

To remediate an issue, you may create an action plan directly from this issue.

For further details, see Managing Action Plans.

Following Up Issues

To view remediated / non-remediated issues:

1. Click **Test > Remediation > Issues**.

2. In the drop-down list, select:
   - "Closed Issues" (whose action plan is closed)
   - "Open Issues"

MANAGING ACTION PLANS

You can set up action plans to improve a control that has been considered unsatisfactory ("fail").

Accessing Action Plans

To access all action plans:

- In the navigation bar, click **Action Plans**.

To access the action plans you need to work on:

1. In the navigation bar, select **Action Plans**.
2. In the drop-down list, select **Action plans to Implement**.

   ☛ *Displays all action plans you need to implement or approve.*

Creating an Action Plan for Testing

To create an action plan:

1. In the navigation bar, select **Testing > Test Plans**.
2. Open the properties of a test.
3. From the drop-down list, select **Work Program**.
4. Select an issue and in its properties, select the **Action Plans** page.
5. Click **New**.
6. Specify the name and click **OK**.
   The action plan is created, as well as its associated workflow.

   ☛ *For more information on action plan workflows, see Action Plan Workflows.*

   ☛ *The action plan also appears in the following menu:* ***Testing > Remediation > Action Plans >Action Plans Remediating Issues.***

See also Characterizing Action Plans.

Characterizing Action Plans

To access action plan properties:

1. See Accessing Action Plans.
2. Open the action plan properties.

Overview

The action plan **Overview** property page displays:

- the main information in the form of an identification card
- the main progression indicators
- the Gantt of actions together with the progress history

> ☛ *You cannot modify this information in the overview page.*

Below are the progress indicators displayed in the dashboard:

- **Progress** (%)

  > ☛ *Corresponds to the value of the **Progress Update Percentage** column of the last progress update (**Progression History** section).*

- **Timing**
  - On Time
  - Overdue

  > ☛ *Corresponds to the value of the **Progress Evaluation** column of the last progress update (**Progression History** section).*

- **Result**
  - Failure
  - Success
  - Unknown

  > ☛ *Corresponds to the value entered in the **Outcome** field of the **Success Factors and Outcome** section.*

General characteristics

You can specify the following information:

- **Name**: action plan name.
- **Priority**: enables indication of a level. Priority can be:
  - "Low"
  - "Medium"
  - "High"
  - "Critical"
- **Owner**: this field is specified by default by the user who created the action plan.
- **Owner Entity**: entity responsible for action plan implementation.
- **Approver**: user responsible for validation of the action plan when all actions are completed.
- **Organizational Level**: final objective of plan; this can be:
  - "Global"
  - "Local"
- **Origin**: enables definition of the context of carrying out the action plan:
  - "Audit"
  - "Compliance"
  - "Event"
  - "Risk"
  - "RFC"
  - "Other".
- **Category**: the action plan can for example be connected to:
  - risk impact reduction
  - project management
  - process improvement
  - control performance improvement
  - etc.
- **Nature**: enables definition of whether the action plan is:
  - Corrective
  - Preventive
- **Means**: text description of means required/desired for action plan execution.
- **Description**: enables to specify additional information on the action plan and its characteristics.
- **Steering Calendar**: used for sending reminders to the person responsible for an action plan so that they can indicate action plan progress.

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

Responsibilities

The user defined as action plan **Responsible** is responsible for definition of actions to be carried out and their execution.

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

Financial assertion

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

Success Factors and Outcome

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

You can enter the **Outcome** of the action plan.

- Unknown
- Failed
- Succeeded

Scope

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

You can connect objects of the following types:

- controls
- Applications
- risks
- entities
- process categories
- process
- incidents
- issues

Progress history

The **Progress History** section enables you to follow-up the progress update history by the action plan owner.

See Indicating Action Plan Progress.

Milestones

Milestones are key dates of the action plan.

☛ *The planned end date is mandatory.*

Attachments

You can attach documents to an action plan or specify an URL.

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

Managing Actions

☛ *See also: Managing Action Plans.*

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

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

Accessing actions

To access the actions of an action plan:

1. In the navigation bar, click **Action Plans**
2. Open the properties of the action plan that interests you.
3. Select the **Actions** page.

Creating actions

To create an action from an action plan:

1. See Accessing actions.
2. In the **Actions** page, click **New**.
3. Select an **Owner**.
4. (Optional) Specify milestones, which are important dates of the action.
   - **Planned Begin Date**
   - **Planned End Date**
5. Click **OK**.

The action is created.

Describing action sequence flow

To describe action sequence:

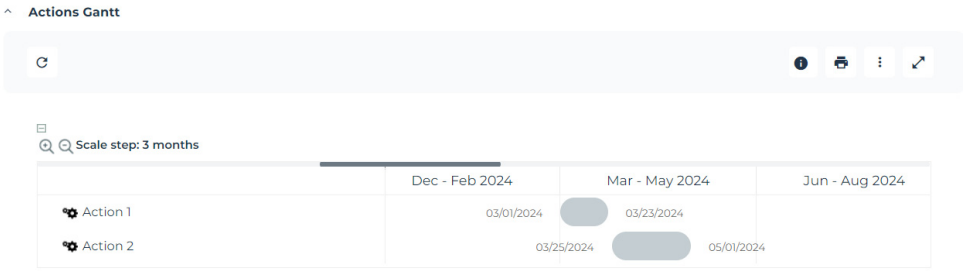
1. See Accessing actions.
2. In the **Next** column, specify the action that comes next.

Viewing the actions Gantt

Hopex enables you to view the planning of actions in the form of a Gantt chart.

To access the actions Gantt chart:

1. See Accessing actions.
   In the lower part of the **Actions** page, the actions Gantt is displayed:



☛ *It is also available in the **Overview** and **Progress report** pages of the action plan.*

Reassigning actions

To reassign several actions:

1. See Accessing actions.
2. In the **Actions** page, select the actions concerned.
3. Click the **Assignment** button that appears.
4. In the wizard, select a **Responsible** user.
5. Click **OK**.

The initial responsible user has been replaced by the one you have just chosen for the concerned actions.

Action Plan Workflows

☛ *See also: Managing Action Plans.*

A workflow is automatically created at creation of the action plan.

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

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

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

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

"Bottom-up" approach

In a "bottom-up" approach, the action plan can be created by any user. An approver must validate the action plan so that it can be implemented. This is the case when

control assessment questionnaire respondents propose an action plan: they must submit it via the workflow.

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

"Top-down" approach

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

Internal controllers carrying out tests use this approach:

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

Action workflow

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

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

☛ *See Action Workflow.*

Indicating Action Plan Progress

☛ *See also: Managing Action Plans.*

When the action plan has been started, you can create progress states to indicate its progress.

To specify action plan progress:

1. In the navigation bar, select **Action Plans > Action Plans > Action Plans to Implement**.
2. Open the properties of the action plan.
3. Expand the **Action Plan Progress** section, and in the **Progress Update** frame, click **New**.
4. Specify a **Progress Update Percentage**.
5. If required, specify the **Progress Assessment**.
   You can specify whether the action plan is:
   - On time, or
   - Late
6. Click **OK**.
   The progress state is created. You can create these at regular intervals.

Action Plan Follow-up Report (Dashboard)

Path

Navigation bar > Reports

Result

This report comprises several charts:

- bar charts
- pie charts

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

Action plans by status

This bar chart presents action plan statuses.

Action plans by progress

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

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

Action plan by priority

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

Possible priorities are the following:

- Critical
- High
- Mean
- Low

Action plans by category

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

Possible categories are as follows:

- Corrective
- Preventive

Action plans by entity

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

- x-axis: all entities
- y-axis: number of action plans linked to each entity and sub-entity

☛ *If no entity is selected, all root entities are taken by default.*

Action plans by process

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

- x-axis: all processes (process categories and processes)
- y-axis: number of action plans linked to each process and sub-process

CONTROL-RELATED REPORTS

This section groups the main reports used in each step of internal control. They can provide help in decision-making and allow you to follow up progress of your work.

- ✓ Control Environment Report
- ✓ Control Impacts Report
- ✓ Control Register Reports
- ✓ Control Execution Reports
- ✓ Control Testing Reports
- ✓ Issue-Related Reports
- ✓ IT Regulatory Compliance Reports

☛ *For more information on reports, see:*

- *Accessing Reports*
- *Creating a Report*

CONTROL ENVIRONMENT REPORT

You can choose to display the following elements for a chosen control:

- the risk context
  - process categories
  - process
  - Applications
  - Org-Units
  - business lines
- the strategic objects impacted by the risk (objectives)
- risk consequences (associated risks)
- preventive controls designed to remediate the risk

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

  An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.
- action plans and actions

Access path

Control properties (**Reporting > Control Environment**)

Report parameters

Parameters	Constraints
Control	Mandatory
Control context (process category, process, application, entity, business line)	Optional
Mitigated Risks	Optional
Deficiencies	Optional
Action plans	Optional
Risk context (process categories, processes, applications, entities, business lines)	Optional

Creating a control environment report

To display a control environment report:

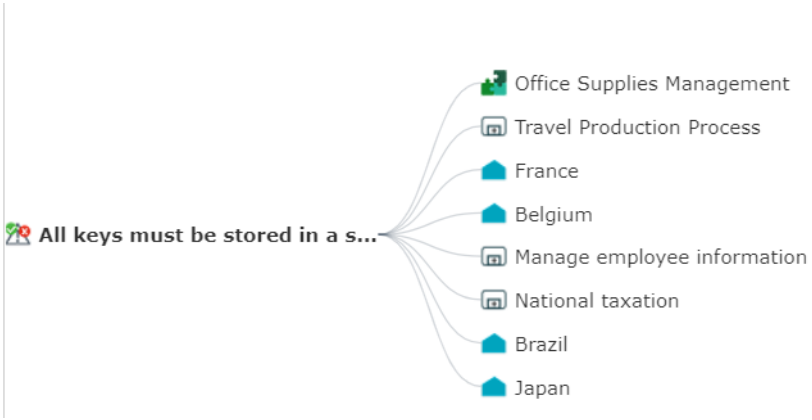
1. In the control properties, select the **Reporting > Control Environment** page.

2. In the **Parameters** section, select the object types you want to display:
   - **Control contexts**
   - **Mitigated risks**
   - **Issues**
   - **Action plans**
   - **Risk contexts**
3. In the **Report Display** field, specify whether you want to display the risk environment objects:
   - in a horizontal fashion, or,
   - in a circular fashion (based on the selected risk)
4. Click **Refresh**.

Using this diagram, you can:

- fold/unfold the branches
- open the properties page of the selected object.

Example



Control Impacts Report

This report is a dendrogram displaying all the elements impacted by a control.

Access path

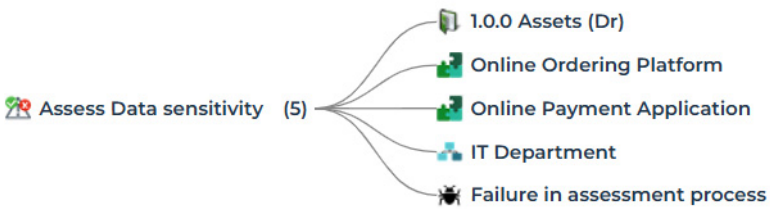
Control property pages:

- **Reporting > Control Impacts**, or
- **Overview**

Report parameter

Parameter	Type of parameter
Control	1 control

Example



CONTROL REGISTER REPORTS

Control Identification (Dashboard)

This report presents distribution of controls according to several perspectives:

- entities
- process categories/processes
- control types
- accounts

Path

Navigation bar > Reports

Parameters

Parameters	Remarks
Begin Date	Optional All controls created after this date are selected
End date	Mandatory Initialized with current date All controls created before this date are selected
Context objects	Optional The context object can be an: - Entity - Control type - Process category/process - Account

Connecting context objects

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

- Entities
- Process categories/Processes
- Types of control
- Accounts

To connect context objects:

- In the appropriate frame, click **Connect** ....
  In the dialog box that appears, you can select objects in two ways:
  - via a tree: select the objects to be connected in the proposed tree and click **OK**.
  - via the query tool: select the required object type in the drop-down list, click the **Find** button, select the objects to be connected and click **OK**.

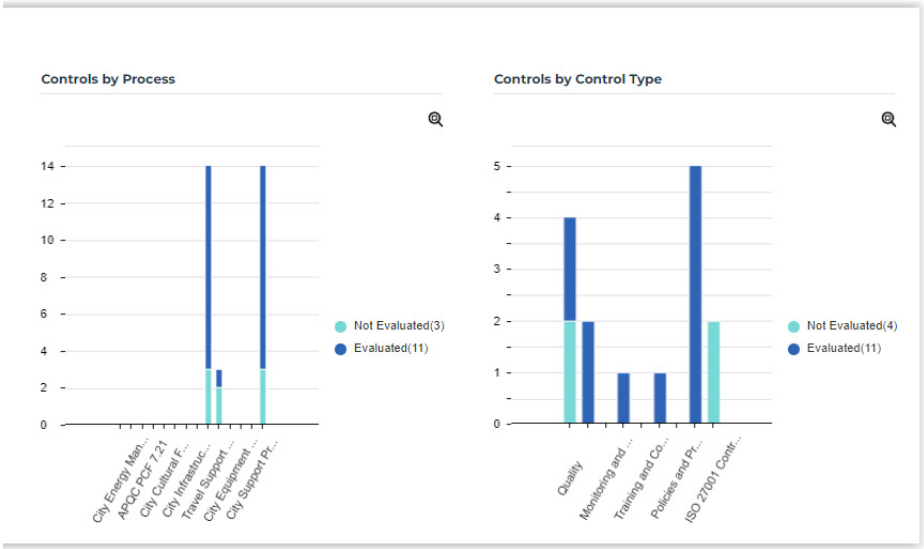
Results

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

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

Bars of the bar chart distinguish assessed controls from those not yet assessed.

Example



CONTROL EXECUTION REPORTS

Consolidated Execution Results

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

Access path

Navigation bar > Reports

Parameters

Parameters
Schedule
Begin Date
End date
Entity type
Entity

Result

The matrix comprises:

- a list of entities: by default, all entities are selected.

  ☛ *If the "Entity type" parameter is specified, selected entities correspond to this specified entity type.*

- a **Total number of controls**: number of controls linked to the entity (or its sub-entities).
- a **Total number of instances**: controls are counted as many times as there are contexts for the same control.

  If a control is assessed in the framework of two different entities, the control is counted twice: **Hopex Internal**

Control distinguishes two instances of the assessed control.

☛ *For more details on control contextualization see Contextualizing Controls.*

- for each month:
  - a **Number of assessed instances**
  - a number of instances considered as satisfactory ("pass")
  - a % of instances considered as satisfactory ("pass")

Example

			Jan-2016			Feb-2016		
	Total Nb of Controls	Total Nb of Instances	Nb of Assessed Instances	NB of OK Instances	% OK Instances	Nb of Assessed Instances	NB of OK Instances	% OK Instances
Belgium	9	9	0	0	0 %	8	0	0 %
France	16	18	0	0	0 %	12	0	0 %
Italy	9	9	0	0	0 %	10	0	0 %
Japan	3	3	0	0	0 %	0	0	0 %
USA	11	11	0	0	0 %	12	0	0 %

Following Up Execution Sessions

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

Access path

This report is available from a particular execution session.

To access this report from an execution session:

1. In the properties of an execution campaign, select the **Sessions** page and open the properties of the session.
2. Select the **Follow-up** page.

Parameters

Parameters
Session

Result

A summary displays general information on the current session.

This report presents charts concerning campaign progress:

- Percentage of completed questionnaires
- Percentage of validated questionnaires
- Distribution of questionnaires by status, for each respondent

CONTROL TESTING REPORTS

Testing Coverage

The testing coverage report provides help in decision-making when selecting tests.

It enables generation of tests.

☛ *See Viewing the test coverage report.*

Plan Synthesis

This report presents an overview of plan indicators.

Path

Plan property page> Reports > Overview

Result

A summary table presents:

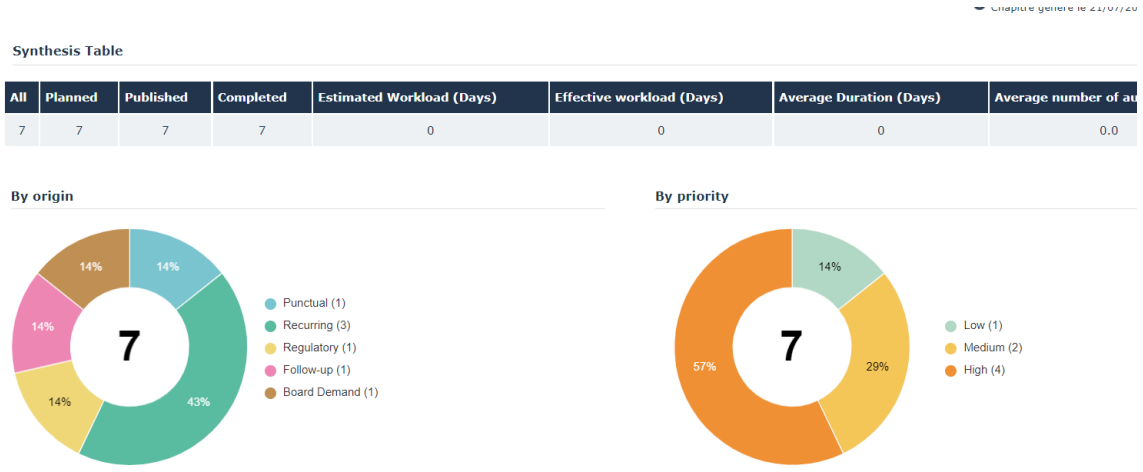
- number of tests (total number, number of tests planned, published and completed)

  ☛ *If you click the figure indicated, the corresponding tests appear at the bottom of the window. You can consult the properties of each test and modify these from this list.*
- estimated and effective workload (in days)
- average duration (days)
- average number of controllers

Charts present the distribution of tests by:

- origin
- priority
- category
- score
- status

Example



Synthesis Table

All	Planned	Published	Completed	Estimated Workload (Days)	Effective workload (Days)	Average Duration (Days)	Average number of au
7	7	7	7	0	0	0	0.0

Other Reports

Reports allow you to follow up progress of a particular object (test plan, test, action plan). There are available on each object in the **Testing** menu of the navigation bar.

Test plan follow-up reports

Reports enable test plan execution follow-up.

☛ *See Displaying test plan follow-up reports.*

Test follow-up report

For more information on possibilities for test follow-up in particular, see:

- Planning tests using a Gantt chart
- Viewing resource availability
- Consulting the work program report
- Generating test reports
- Test expenses reports
- Supervising Tests
- Test assessment reports

Action plan report

To follow up progress of an action plan in particular, see Following up action plan progress.

ISSUE-RELATED REPORTS

Issues by Remediation Status

The issue follow-up report is presented in the form of a pie chart.

Path

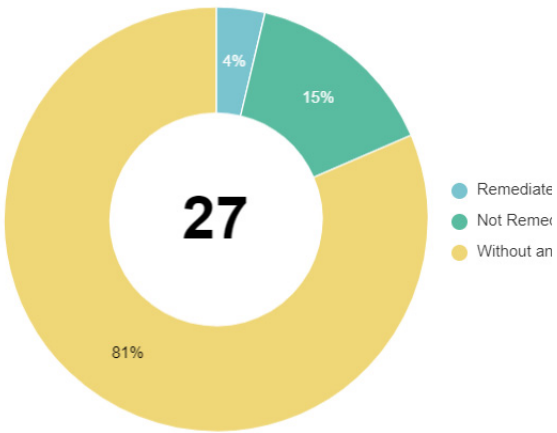
Navigation bar > Reports

Result

This report distinguishes issues:

- **Remediated**: issues with an action plan whose status is:
  - Completed
  - Closed
- **Non-Remediated**: issues with an action plan of which status is:
  - To send
  - To start
  - Under follow-up
- **Without action plan**

Example



Issues by Impact

This report is a pie chart that groups issues by impact (very low, medium, high, very high)

You can filter results:

- by issue status (open, closed)
- by control type impacted by the issue.

Use case:

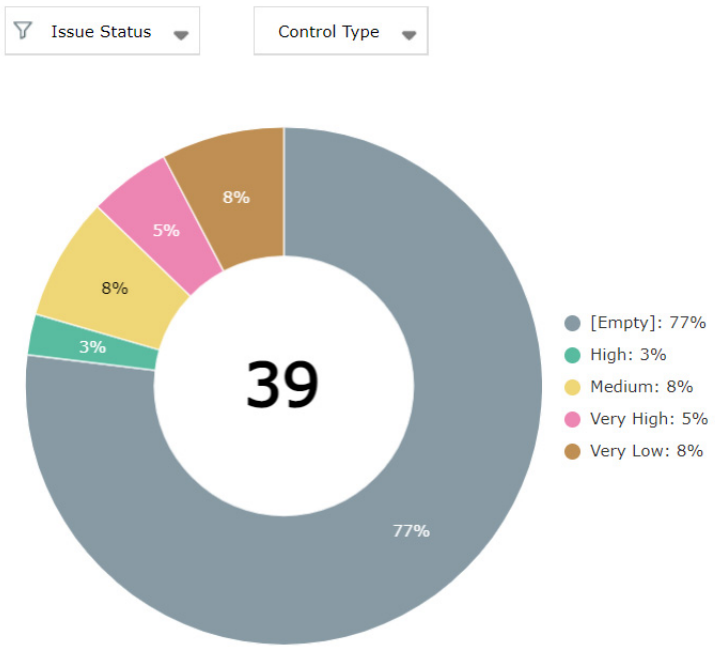
- You have connected a number of controls to a control type to meet specific requirements (for example, "IT Compliance")

- This report enables you to view the issues that impact the control type of interest.

Path

Navigation bar > Reports

Result



HOPEX ENTERPRISE RISK MANAGEMENT

User Guide

Hopex Aquila

CONTENTS

Contents

MANAGING RISKS

To control risks, it is necessary to identify and qualify the risks encountered in the execution of a process.

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

When risks have been analyzed and assessed, management determines how each of these risks should be treated. **Hopex Enterprise Risk Management** offers tools that simplify creation and analysis of risks to identify the most important of these and set up adapted corrective or preventive actions.

The following points are covered here:

- ✓ Risk Management Profiles
- ✓ Creating a Risk
- ✓ Risk characteristics
- ✓ Listing Risks
- ✓ Risk Workflow

RISK MANAGEMENT PROFILES

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

Profiles	Tasks
Risk Manager (Or GRC manager)	The Risk Manager is responsible for executing the following tasks on risks within his responsibility domain: - identifying risks - carrying out direct assessments - managing assessment campaigns - defining action plans - analyzing and following report creation
GRC Contributor	- answering assessment questionnaires - define action plans See The GRC Contributor Desktop.

☛ *For more details, see also Accessing the GRC Desktop.*

CREATING A RISK

To create a risk:

1. In the navigation bar, select **Risks**.
2. Click **New**.

   ☛ *You may also create a risk from the home page (**Quick access > Actions > Create a Risk**.*
3. Enter a **Name**
4. (optional) Specify the risk **Identification Mode**
   The risk could have been identified from:
   - an "incident database"
   - a "workshop"
   - a "survey"
   - an "audit"
5. (optional) Enter a **Description**
6. Click **OK**.

You can complete risk description through the risk property page.

See:

- Risk characteristics
- Risk Workflow

RISK CHARACTERISTICS

☛ *To access risks, see Listing Risks.*

☛ *To be able to assess risks in the framework of assessment campaigns by questionnaires, you must first specify certain properties. For more details, see Preparing the Assessment Environment.*

General characteristics

To access characteristics of a risk:

❱ Click a risk in the list of risks.

In the property page, you can specify:

- the risk identification **Code**
- the fact that risk is "high level" by selecting the **Major Risk** check box
- the risk **Owner**
- the risk **Identification Mode**
  The risk could have been identified from:
  - an "incident database"
  - a "workshop"
  - a "survey"
  - an "audit"
- the risk **Description**

☛ *The risk **Status** cannot be modified since it is managed by the workflow associated with the risk.*

See also:

- Analyzing Risks
- Risk Responsibilities (RACI)
- Risk Overview
- Defining the Scope of a Risk (scoping risks)

Risk Overview

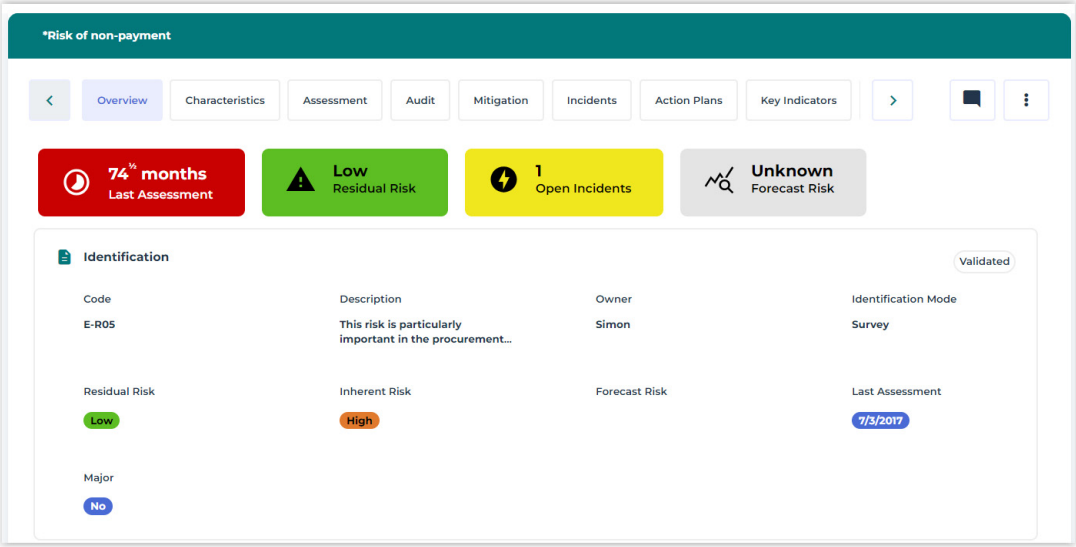
☛ *To access risks, see Listing Risks.*

The **Overview** property page gives access to:

- A riskl card, which gives an overview of the main risk characteristics

  ☛ *For more details, see Card of an Object in the "Platform - Common Features" section.*

- Computed information in the form of a dashboard



Here is the computed information in the form of a dashboard:

- **Last Assessment**: elapsed time (number of months) since the last assessment (either direct assessment or through campaigns)

  ☛ *This is an indicator of how often a risk is assessed. This can be useful when it comes to decide when to perform the next assessment.*

- **Residual Risk**: average of the net risk obtained from the last assessment session. All the contexts for which the risk was assessed during the last assessment session are considered (e.g. entities, processes, applications…) and the average is computed.

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

- **Open Incidents**: number of incidents corresponding to risks having a status other than "closed".

  ☛ *See the Collecting Incidents guide for more details on incidents.*

- **Forecast risk**: represents the residual risk forecast for the year to come (average residual risk)

Risk Responsibilities (RACI)

☛ *To access risks, see Listing Risks.*

Risk properties include a **Responsibilities** section to define the different persons responsible for risk management. For more details, see Responsibilities (RACI).

Note that the Risk Assessor, who answers risk-related questionnaires, is to be specified in the properties of the entity connected to the risk(Entities / Processes/).

☛ *For more details, see:*

- *Prerequisites to Risk Assessment*
- *Specifying responsibilities within an entity.*

See also:

- Defining the Scope of a Risk
- Analyzing Risks
- Risk Overview

Defining the Scope of a Risk

Contextualizing a risk consists in defining its scope.

To define the scope of a risk:

❱ In the risk properties, expand the **Scope** section.

The scope can consist of different types of objects:

- **Process categories** and **Processes** exposed to the risk. See Managing Process Categories and Processes.

  🕮 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

  🕮 *A process describes how to implement all or part of the process required to make a product or handle a flow.*

- **Operations**

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

- **Entities** concerned by the risk. See Managing Entities.

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

  ☛ *Defining entities on risks is a pre-requisite to risk assessment. See also Preparing the Assessment Environment.*

- **Objectives** expected related to risk management.

  🕮 *An objective is a goal that a company or organization wants to achieve, or is the target set by a process or an operation. An objective*

allows you to highlight the features in a process or operation that require improvement.

- **Applications**. See Managing Applications.

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

- **Business Lines**: See Managing Business Lines.

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

Analyzing Risks

The aim of risk analysis is to obtain a good understanding of risks. You need to take into account:

- risk causes
- positive or negative risk consequences

The risk analysis phase associates a risk with:

- risk types
- risk factors
- consequences
- other risks

To analyze a risk:

1. See Listing Risks.
2. Select a risk and open its properties.
3. In the **Characteristics** tab, expand the **Analysis** section.
   A risk is characterized by:
   - **Risk Types**: for more details, see Risk types.

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

   - **Risk Factors**: for more details, see Risk Factors.

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

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

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

   - **Related Risks**

     *The incidents related to the risk appear in the **Incidents** page of the risk properties.*

Risk types

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

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

To create your own risk types:

1. In the navigation bar, click **Risks > By Risk Type**.
2. Click **New**.
3. Enter the name of the risk type and click **OK**.
   The new risk type appears in the navigator menu tree.

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

Risk Factors

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

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

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

Risk consequences

To define consequences associated with a risk:

1. See Listing Risks.
2. In the risk properties, **Analysis** section, **Risk Consequences** tab, click **New**.

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

Viewing Audit Recommendations Connected to a Risk

To view risk-related recommendations:

1. See Listing Risks.
2. In the properties of a risk, select the **Audits** page.

   ☛ *This page is available if:*

   - *you have the **Hopex Internal Audit** solution*
   - *You are "Audit director" or "GRC functional administrator".*

This page contains:

- Recommendations that have the risk in their scope
- Recommendations connected to a finding with the risk in its scope

For more details on risks and recommendations within the framework of an audit, see:

- Defining and Assessing Risks Detected during the Audit
- Sending Recommendations

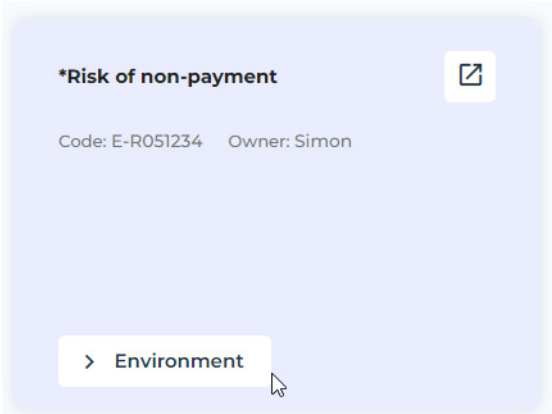
Browsing a Risk Environment

To browse the objects of the risk environment:

1. See Listing Risks.
2. In the list of risks, click **Browse**.

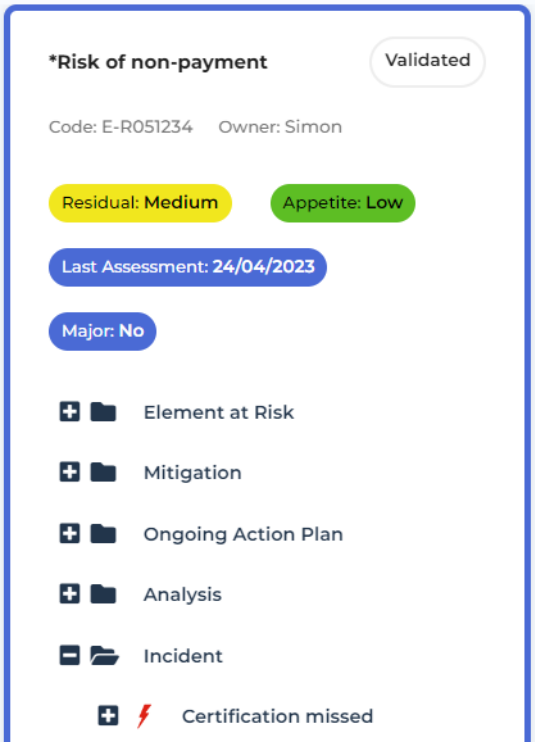
Cards are available for each risk.

3. Hover the mouse over a card and click **Environment**.



The objects of the risk environment are displayed in trees. They form the risk extended scope.

- **Elements at Risk** (for example: process)
- **Mitigation** elements (controls)
- **Ongoing action plans**


*Risk of non-payment
Validated
Code: E-R051234
Owner: Simon
Residual: Medium
Appetite: Low
Last Assessment: 24/04/2023
Major: No
Element at Risk
Mitigation
Ongoing Action Plan
Analysis
Incident
Certification missed

LISTING RISKS

Accessing All Risks

To access risks:

❱ In the navigation bar, select **Risks**.

For each risk, you can access the following information:

- **Code**
- **Status**

  ☛ *The **Status** enables you to distinguish between risks that were **Submitted** (and need to be reviewed) from those that were **Validated**.*
- **Major Risk** (is it a major risk or not?)
- **Entities**
- **Last assessment** (date)
- **Inherent risk**

  🕮 *The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact.*
- **Residual risk**

  🕮 *The residual (or net) risk indicates the risk to which the organization remains exposed after management has processed the risk.*
- **Open Incidents** (number of)
- **Forecast Risks** (number of)
- **Action Plans** (number of)

Listing Risks by Risk Types

To list risks by risk types:

❱ In the navigation bar, click **Risks > By Risk Type**.

This list displays all Risks in your environment in a tree structured around Risk Types.

For each risk type, columns display the number of **Risks**.

For each risk the following information is displayed in columns:

- Associated **Entities**
- **Last assessment**
- **Residual risk**

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

- **Forecast risk**

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

  Other columns are available but not displayed by default. You can add them.

Accessing Orphan Risks

To access risks that are not connected to any contexts (orphan risks):

1. See Accessing All Risks.
2. From the **Risks** drop-down list, select **Orphan risks**.

This list displays all the risks that have no impact on the organization. These risks are not connected to any processes, applications, entities or business lines.

*To specify the risk impact, fill in the **Scope** section of risk characteristics.*

Accessing Materialized Risks

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

To access risks that materialized through an incident:

1. See Accessing All Risks.
2. From the **Risks** drop-down list, select **Materialized risks**.

RISK WORKFLOW

The risk creation process is managed by a workflow. Only certain profiles are authorized to create, submit, validate or reject a risk.

☛ *For more details on the risk creation workflow, see Risk Workflows.*

Risk validation steps

The steps in the validation process of a new risk are the following:

- Having specified the characteristics of a new risk, the risk creator (who is also the risk owner) must **Submit** the risk.
- When a risk has been submitted, the Risk Manager can:
  - **Validate** the risk (it takes the "Validated" status).
    A notification is sent by mail to the user defined as "Owner".
  - **Reject** the risk.
    In this case, the risk takes status "Rejected", but is not deleted.

Validating or rejecting a risk

To validate or reject a risk:

1. See Accessing All Risks.
2. From the **Risks** drop-down list, select **Risks to review**.
3. Select the risk and use the **Workflow** button to validate or reject it.

☛ *You can also select several risks to perform a mass transition.*

ASSESSING RISKS

After having identified and analyzed the risks encountered by the enterprise, it is essential to highlight the most important of these in order to remediate them.

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

- ✓ Risk Assessment Types
- ✓ Prerequisites to Risk Assessment
- ✓ Risk Direct Assessment
- ✓ Viewing and Analyzing Risk Assessment Results

Risk Assessment Types

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

- impact
- likelihood
- risk control level

Direct Assessment or Assessment by Campaign

Risks can be assessed:

- individually, in the risk properties: see Creating a Direct Assessment on a Risk.
- simultaneously, via the interactive heatmap: see Assessing Multiple Risks Simultaneously.
- Through an assessment questionnaire sent to appropriate recipients: see Starting an Assessment Campaign.

> ☛ *Questionnaires sent within the framework of campaigns are displayed in the form of a heatmap.*

Results of risk assessment can be displayed in dedicated reports which make it easier to analyze the assessed risks. For more details, see Risk-Related Reports.

> ☛ *See also: Prerequisites to Risk Assessment.*

Risk Assessment Templates

Hopex offers two perspectives for risk assessment:

- Risk Assessment by Entity and Process
- Risk Assessment by Application

> ☛ *See also: Prerequisites to Risk Assessment.*

PREREQUISITES TO RISK ASSESSMENT

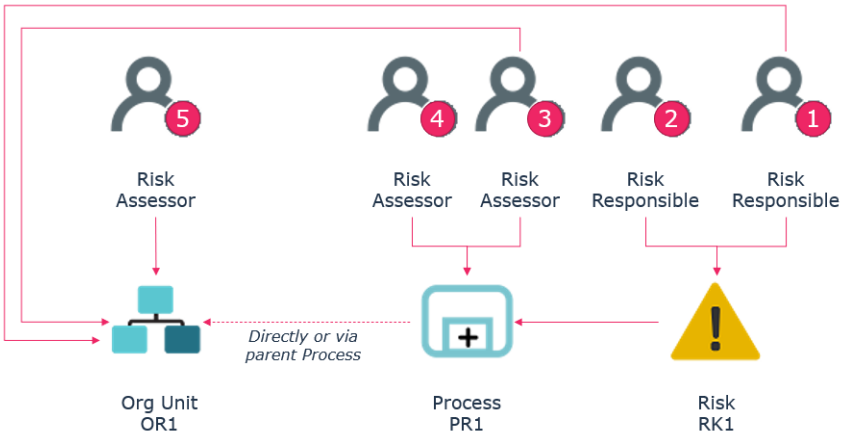
"Risk Assessment by Entity and Process" Template

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

- connected risks to at least one entity/ one business process
- specified one or several respondents in the entity/process properties (Risk assessor)

Respondents to risk-related questionnaires can be defined on:

- entities
- processes connected to entities (directly or via a parent process)
- risks connected to processes (directly or via a risk)



Respondent definition logics

"Risk Assessment by Application" Template

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

- connected risks to at least one application
- specified one or several respondents in the application properties (Application owner)

RISK DIRECT ASSESSMENT

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

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

- in risk properties: Creating a Direct Assessment on a Risk
- globally, via a heatmap:Assessing Multiple Risks Simultaneously

Direct assessment is carried out for all entities or applications available in the **Scope** section of the risk properties.

☛ *See also: Starting an Assessment Campaign.*

Direct Risk Assessment Templates

Hopex Enterprise Risk Management provides risk assessment templates in the context of the following objects:

- entity and process
- application

Assessed characteristics

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

Example of assessed characteristics:

- Impact
- Likelihood
- Control Level

  📖 *Risk control level enables characterization of control efficiency in mitigating the risk.*
- Residual risk

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

Respondents

Respondents can be:

- Risk ***Responsible*** users (on risks), or
- ***Risk Assessors*** (on entities or processes)

☛ *It is possible to define several respondents.*

☛ *For more details, see Prerequisites to Risk Assessment.*

Questionnaire

The questionnaire relates to characteristics to be assessed for all risks determined as objects of assessment:

- Impact
- Likelihood
- Control Level

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

Creating a Direct Assessment on a Risk

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

This is an assessment by an expert.

To create a direct assessment on a risk:

1. Select the risk and open its properties.
2. Select the **Evaluation** page.
3. Click **New Assessment**.

   > ☛ *A page offering to select context(s) appears if several contexts are available for the risk concerned.*

4. Assign characteristics values for the risk being assessed:
   - **Impact**: the impact of the risk when it occurs.
   - **Likelihood**: the probability that the risk will occur.

     > ☛ *If the risk has already been assessed, impact and likelihood values from the last assessment are suggested. You can modify these values for the new assessment.*

   - **Control Level**

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

     > ☛ *If the risk has already been assessed, a Control Level value is also suggested. For more information, see Risk Control Level.*

5. Specify the **Assessment Date** if necessary.
6. Click **OK**.
   An assessment is created.

Assessing Multiple Risks Simultaneously

You can assess several risks simultaneously via an ***interactive heatmap***.

To assess several risks simultaneously:

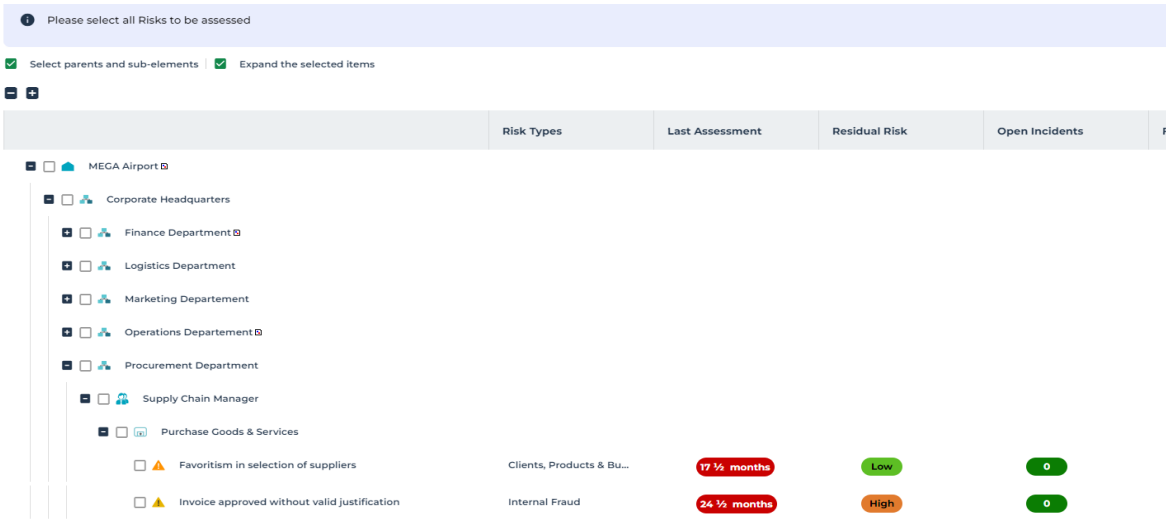
1. In the navigation bar, click **Assessment > Direct Assessment > Risk Multiple Assessment**.
2. Click **New Assessment**.

3. In the window that appears, select the **Assessment template**:
   - **Risk Assessment by Entity and Process**
   - **Assessment of risks by application**
4. In the displayed tree, select the objects that define the assessment context (entity or application, depending on the selected template).

   ☛ *A risk is assessed in the context of elements of the branch from the risk up to the root.*

   To help you choose the risks to be assessed, the following information is displayed in columns:
   - **Risk types**
   - **Last assessment**
   - **Residual risk**
   - **Open Incidents**
   - **Forecast risk**

   ☛ *This information is also available in the risk dashboard. For more details, see Risk Overview.*



In the example below, if you select the "Procurement Department", the following objects are also selected:
- all the risks and context objects at a lower level
- all parent context objects up to the root of the tree.

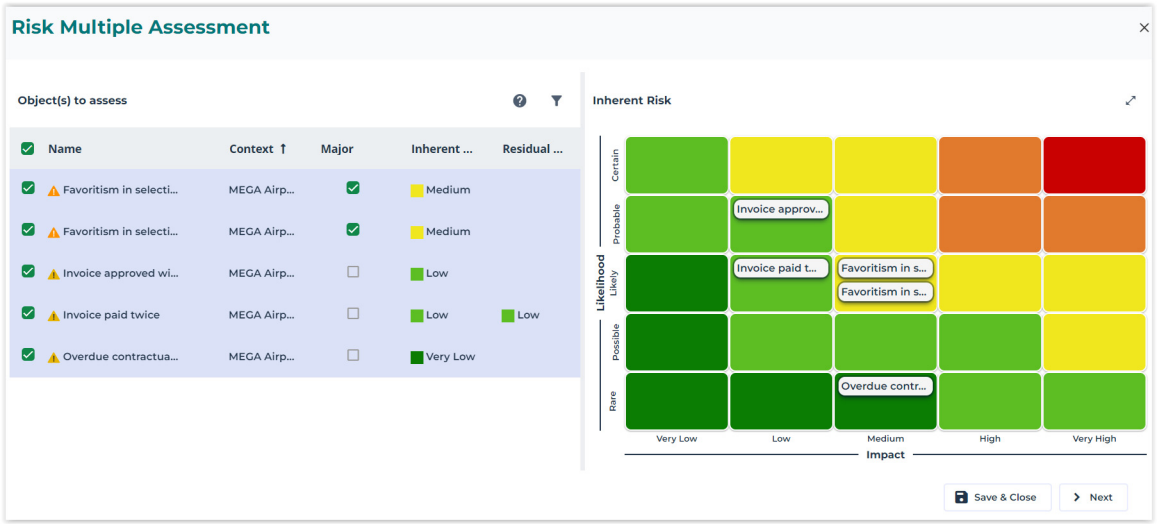
☛ *If you deselect a node of a branch, only the child elements of this branch are deselected.*

☛ *If assessments have already been carried out, the most recent assessment values are presented in columns.*

5. Click **Next**.
   A summary of the assessment appears, enabling you to have an **Overview** of the objects you are going to assess.
6. Click **OK**.
   A heatmap appears. It enables to assess risks visually.

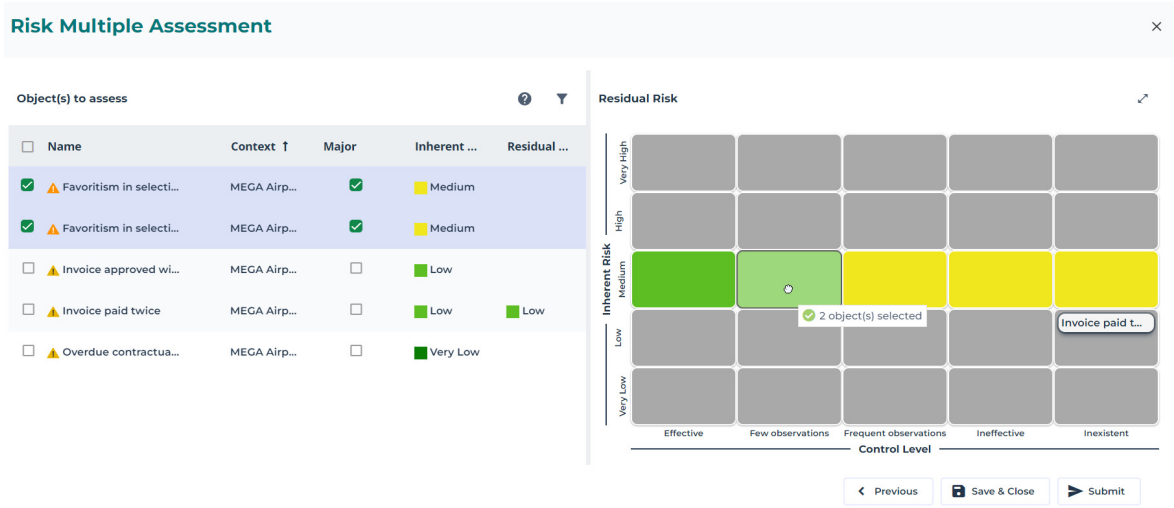
7. (first screen) Position the risks on the heatmap so as to specify:
   - the **Impact** (from very low to very high), vertically
   - the **Likelihood** (from rare to certain), horizontally

   ☛ *Values entered during the last assessment are displayed.*



8. Click **Next**.
9. Specify the **Control Level** (from effective to inexistent).

   ☛ *Vertically, you find the **Inherent risk**, which was computed in the previous screen.*



10. When done, click **Submit**.

You may also choose to close the questionnaire to come back to it and resume the assessment later on (**Save for later**). In this case, the questionnaire is saved in the **Ongoing direct assessments** list.

☛ *For more details, see Using Heatmap Questionnaires in the Common Features section.*

When submitting, an assessment is created in the **Assessment** page of the risk properties.

Click below to view the procedure as a video:

VIEWING AND ANALYZING RISK ASSESSMENT RESULTS

Displaying Risk Assessment Results

To display the results of assessments performed on a risk:

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

> ☛ *The GRC functional administrator only can delete assessment results (that is to say assessment nodes).*
>
> *To delete an assessment node, select it and click **Delete**.*

For each assessment node the following values are computed:

- inherent risk

  > 🕮 *The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact.*

- residual risk

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

Generating Reports on Assessments

Instant reports

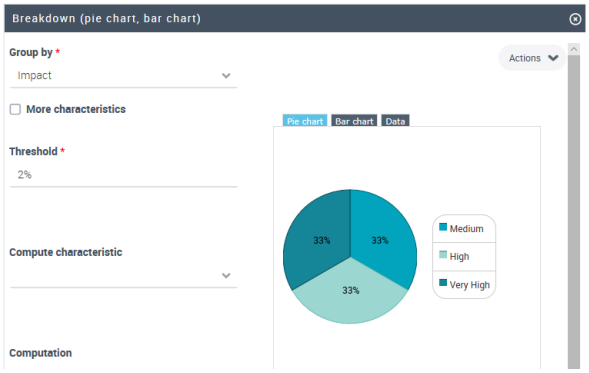
Instant reports provide statistical graphic analysis of the data. You can generate instant reports on a selection of assessments in order to view certain data graphically or to compare the assessments for specific characteristics.

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

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

Example

Find below an example of breakdown report on risks. From the selected characteristics (risk impact in this example), this report offers a graphical representation of results.



For more information on instant reports, see Managing Instant Reports.

Generating dedicated reports

In addition to instant reports, **Hopex Enterprise Risk Management** provides dedicated report templates that facilitate the analysis of the assessed risks. For more details, see Risk-Related Reports.

RISK MITIGATION AND REMEDIATION

Hopex Enterprise Risk Management enables to define risk-mitigating strategies and to implement action plans to remediate risks.

- ✓ Mitigating Risks
- ✓ Remediating Risks

MITIGATING RISKS

To define the risk-mitigation strategy:

1. In the navigation bar, select **Risks.**
2. In the properties of a risk, select the **Mitigation** page.
3. Specify:
   - your risk-mitigation **Strategy**.
   - preventive, detective and corrective **Controls**.

Specifying the Risk-Mitigation Strategy

To define the risk-mitigation strategy:

- In the **Strategy** section of the **Mitigation** page of risk properties, define the strategy that enable to face the risk:
  - ***Acceptance***
    This is the strategy of risk management that consists of accepting the risk having considered its consequences. As long as no desire to remediate the risk is expressed, this strategy will not protect the organization against the risk.
  - ***Reduction***
    Risk frequency can be reduced by installing additional controls, or the impact of its consequences can be reduced if the risk occurs.
  - ***Transfer*** (sub-contractor)
    The risk can also be shared with other partners, in particular when they have greater skills in controlling the risk.
  - ***Insurance***
    Complementing all previous approaches, it is often necessary to seek assurance, in particular for risks of low frequency but with high impact.

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

Specifying Risk Appetite

To specify the level of risk accepted by the organization:

- In the **Strategy** section of the risk **Mitigation** page, define the strategy that enables to face the risk.

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

Implementing Controls

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

To define controls on the risk:

1. In the risk properties, select the **Mitigation** page.
2. In the **Controls** section, define corrective or preventive controls.

☛ *The control nature (corrective or preventive) is to specified in the control properties.*

- *Implementation of prevention controls to reduce risk frequency and impact can be a solution for risk reduction.*
- *Implementing corrective controls enables to bring risk level to an acceptable level.*

REMEDIATING RISKS

To specify action plans that enable to prevent or treat the risk:

1. In the **Hopex GRC** desktop, select **Registers > Risks > All Risks**.
2. In the properties of a risk, select the **Action Plans** page.

> 🕮 *An action plan comprises a series of actions, its objective being to reduce risks and events that have a negative impact on company activities.*
>
> ☛ *For more information on action plans, see Using Action Plans.*

This page contains the list of implemented action plans: for example for creation or improvement of a control, management of a crisis linked to occurrence of an incident, or revision of a process with a view to its improvement.

A workflow is automatically created at creation of the action plan. For futher details, see Action Plan Workflows.

RISK-RELATED REPORTS

Different report templates proposed as standard by **Hopex Enterprise Risk Management** enable analysis of risks and risk types.

☛ *You can create reports from these report templates via the **Reports** menu of the navigation bar. For more details, see Creating a Report.*

- ✓ Risk Environment Report
- ✓ Risk Impacts Report
- ✓ Risk Type Impact Breakdown
- ✓ Bow-Tie Analysis
- ✓ Risk Profile Analysis by Context
- ✓ Aggregation Reports
- ✓ Risk Follow-Up Reports
- ✓ Risk Management Effectiveness Reports

RISK ENVIRONMENT REPORT

☛ *This report is available to all ERM profiles.*

You can choose to display the following elements for a chosen risk:

- the risk context
  - process category
  - process
  - Applications
  - Org-Units
  - business lines
- the strategic objects impacted by the risk (objectives)
- risk consequences (associated risks)
- preventive controls designed to remediate the risk

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

  📖 *An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.*
- action plans and actions

Access path

Risk properties (**Reporting > Risk Environment**)

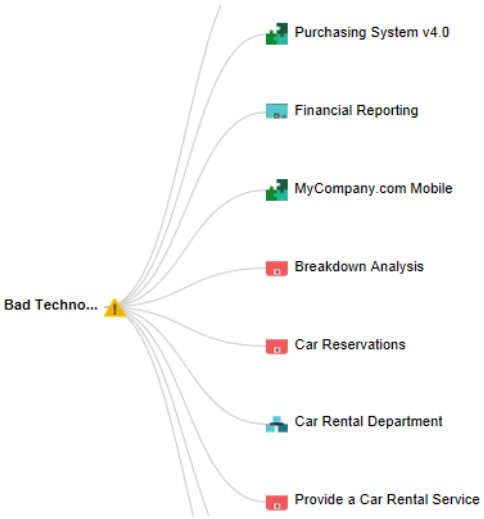
Report parameters

Parameters	Parameter type	Constraints
Risk	1 risk	Mandatory
Risk context (process categories, processes, applications, entities, business lines)	Check Box	Optional
Objectives	Check Box	Optional
Associated Risks	Check Box	Optional
Controls	Check Box	Optional
Incidents	Check Box	Optional
Findings	Check Box	Optional
Action plans	Check Box	Optional
Actions	Check Box	Optional

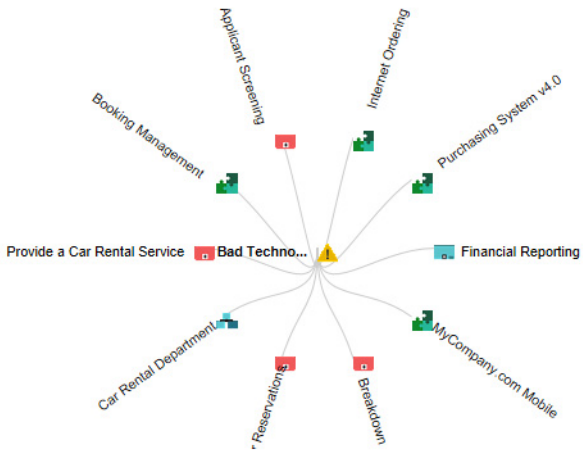
Creating a Risk Environment Report

To display a risk environment report:

1. In risk properties, select the **Reporting > Risk Environment** page.
2. In the **Parameters** section, select the object types you want to display.
3. In the **Report Display** field, specify whether you want to display the risk environment objects:
   - in a horizontal fashion, or,



   - in a circular fashion (based on the selected risk)



4. Click **Refresh**.

Using this diagram, you can:

- fold/unfold the branches
- open the properties page of the selected object.

RISK IMPACTS REPORT

This report is a dendrogram displaying the elements impacted by a risk.

Access path

Risk property pages:

- **Reporting > Risk Impacts**, or
- **Overview**

Report parameter

Parameter	Parameter type
Risk	1 risk

Example

Risk Type Impact Breakdown

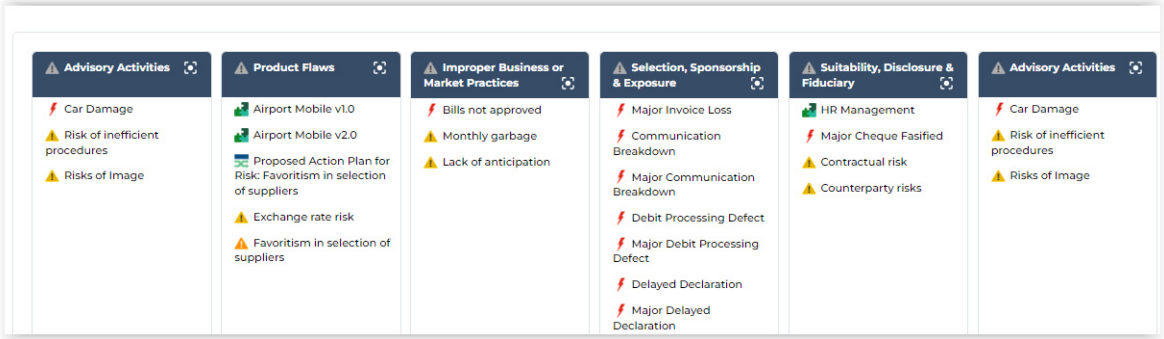
The "Risk type impact breakdown" report enables you to view the impacts of the selected risk type.

To access this report:

1. In the navigation bar, click **Risks > By Risk Type**.
2. Open the risk type properties and select the **Reporting > Risk Type Impact Breakdown** page.

You may:

- Filter the object types to display (risk, application, control, incident, action plan)
- Select a time period



☛ *For more information on breakdown reports, see Handling a Breakdown Report.*

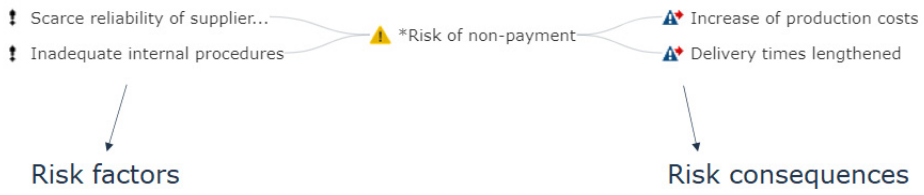
BOW-TIE ANALYSIS

Bow-tie analysis enables to display risk causes and consequences.

Access path

Risk properties (**Reporting > Bow-Tie Analysis**)

Example



Risk Profile Analysis by Context

The report displayed in the form of a dashboard enables to identify risks. It displays the distribution of risks according to several perspectives: by process, by risk type, by entity and by objective.

Access path

Navigation bar > Reports

Report parameters

This consists of selecting risks that will be presented by specifying elements that define their scope: risk types, entities, processes or objectives.

Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default
Scope risk type	Risk type	Not mandatory.
Scope entities	entity	Not mandatory.
Scope processes	process	Not mandatory.
Scope objectives	objectives	Not mandatory.

Report Content

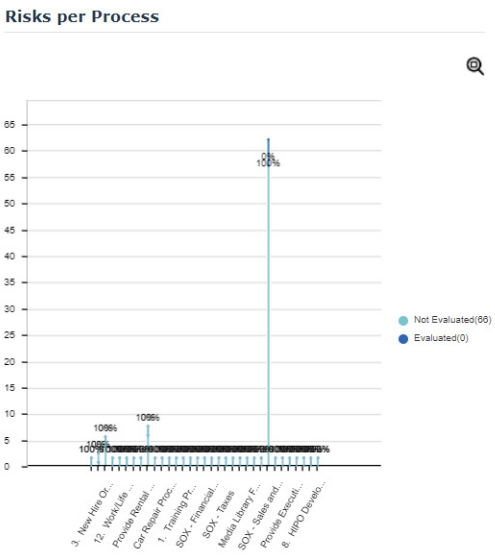
The higher part displays the distribution of risks:

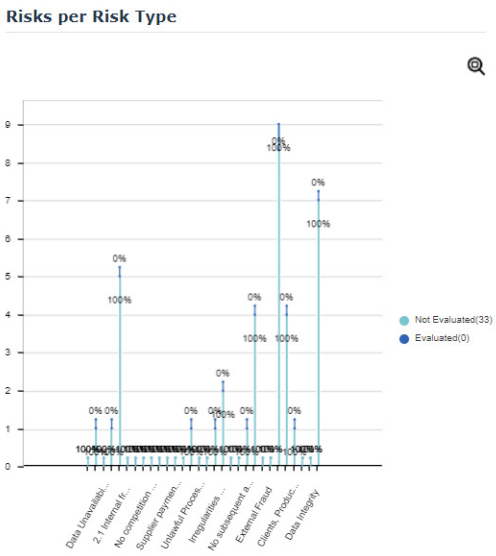
- By process (assessed/not assessed)
- By risk type (assessed/not assessed)
- By entity (assessed/not assessed)
- By objective (assessed/not assessed)
- By status (created, submitted, validated, rejected)

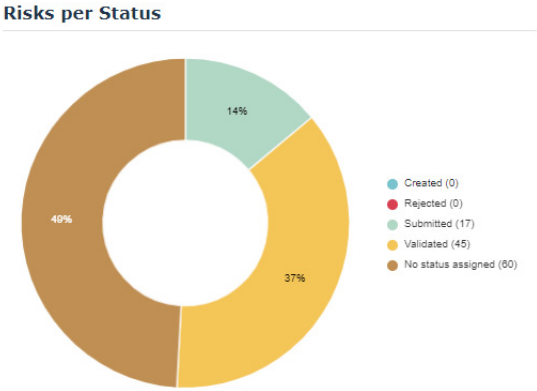
The lower part of displays the distribution of risks based on the following criteria:

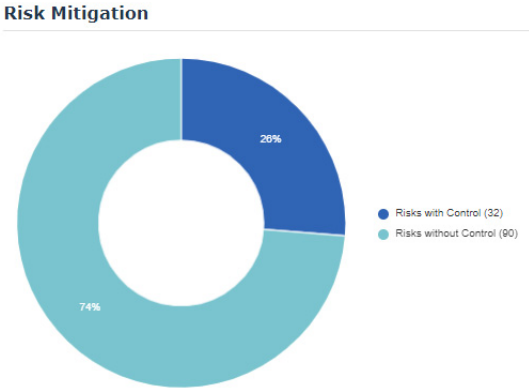
- Risk treatment (risks with/without controls)
- Risk assessment (assessed/not assessed)
- Risk declaration per year

Examples









To obtain a list of risks making up a sector or a barchart bar:

- Click the sector (or barchart bar) that interests you.
  The list of risks taken into account is presented at the bottom of the edit area.

> ☛ *For more details on instant reports, see **Hopex Common Features**.*

AGGREGATION REPORTS

Residual Risk by Risk Type

This report presents in the form of a stacked bar chart:

- on the horizontal axis: the number of risks by risk type

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

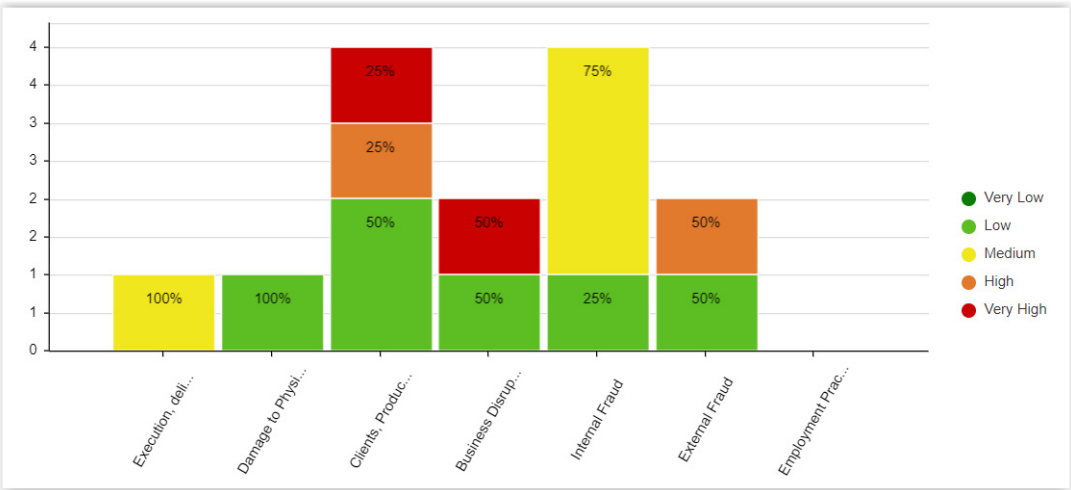
- on the vertical axis: the number of risks by residual risk level

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

Access path

Navigation bar > Reports

Example



Inherent and Residual Risk Heatmap

This report enables the Risk Manager as well as all contributors to display the impact and the likelihood of a set of risks. The objective is to view the risks which require attention.

☛ *Aggregation consists of calculating an aggregated value of the values specified on each risk based on assessments.*

Access path

Navigation bar > Reports

Report parameters

To specify the report parameters:

- After creating the report, in the **Parameters** tab, specify the **List of Risks** that will populate the report.

Heatmap content

This heatmap displays the aggregated values of risks without risk duplication (as context is not taken into account).

Inherent and Residual Risk Heatmap by Context

This report displays distribution of risks according to different criteria:

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

Access path

Navigation bar > Reports

Report parameters

This consists of defining report input data.

Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default.
List of risk types	Risk type	Not mandatory.
List of org-units	entity	Not mandatory.
List of processes	process	Not mandatory.
List of objectives	objectives	Not mandatory.
List of control systems	Control systems	Not mandatory.

☛ *If you complete a risk type and and entity, you get the risks connected to this risk type OR this entity (The OR operator is used here, not AND).*

☛ *To activate control systems, from the main menu select **Settings > Options** then **Compatibility > HOPEX Solutions > Control Systems activation**.*

Report example

Inherent Risk

Impact

Likelihood	Very Low	Low	Medium	High	Very High
Certain	0	0	0	0	0
Probable	0	1	3	2	1
Likely	0	1	1	1	0
Possible	0	3	1	0	0
Rare	0	0	2	0	0

Residual Risk

Control Level

Inherent Risk	Effective	Few observations	Frequent observations	Ineffective	Inexistent
Very High	0	1	0	0	0
High	1	1	1	1	2
Medium	1	1	1	1	0
Low	2	1	1	0	1
Very Low	0	0	0	0	0

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

Risk Assessment by Context

This report enables to display risk assessment results by:

- process category
- objective
- org-unit
- Risk type

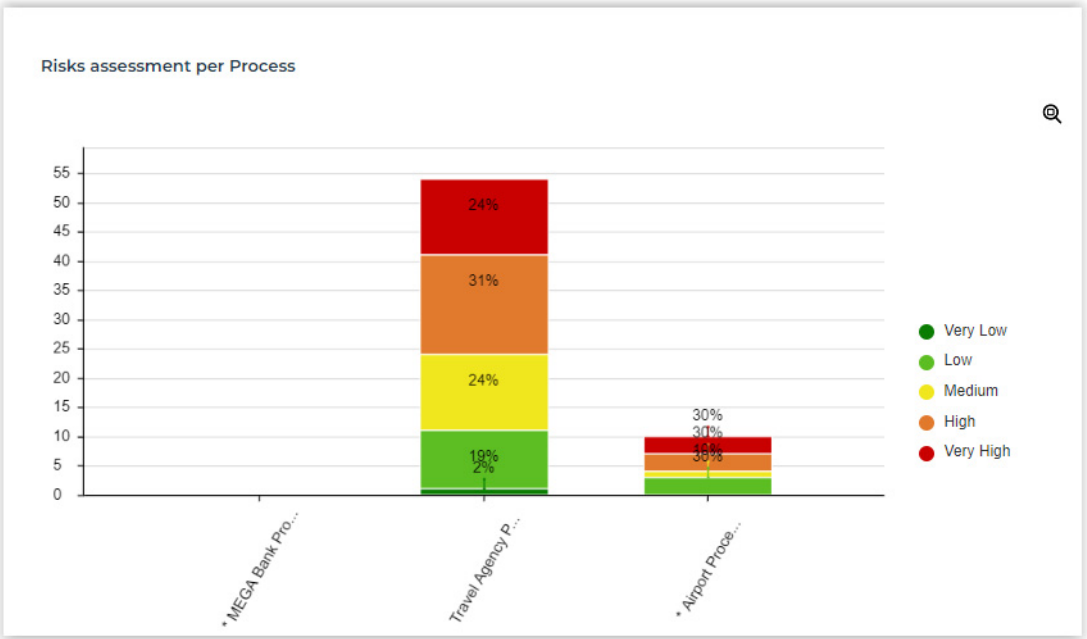
Access path

Navigation bar > Reports

Report parameters

Parameters	Parameter type
Begin Date	Date
End date	Date
Context type	Process category Objective Org Unit Risk Type

Example



Overall Risk Level by Process

This report displays a table of risks linked to the objectives of process categories specified as a parameter.

It displays values of residual risk for each risk in each process category.

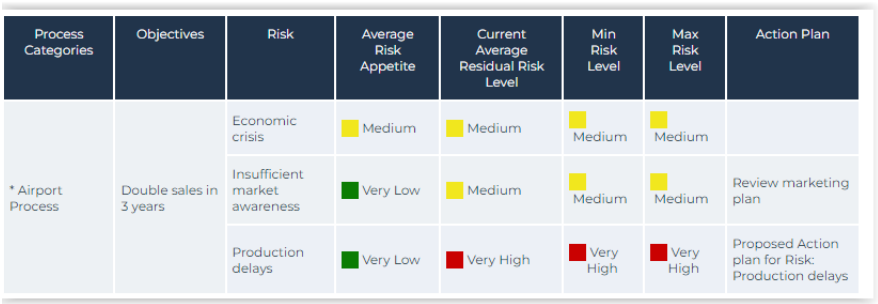
Access path

Navigation bar > Reports

Report parameters

Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory
End date	Date	Current date by default
List of process categories	Process category	Not mandatory

Report example



Process Categories	Objectives	Risk	Average Risk Appetite	Current Average Residual Risk Level	Min Risk Level	Max Risk Level	Action Plan
* Airport Process	Double sales in 3 years	Economic crisis	Medium	Medium	Medium	Medium	
		Insufficient market awareness	Very Low	Medium	Medium	Medium	Review marketing plan
		Production delays	Very Low	Very High	Very High	Very High	Proposed Action plan for Risk: Production delays

Overall Risk Level by Entity

This report displays a table of risks linked to the objectives of entities specified as a parameter.

It displays values of residual risk for each risk in each entity.

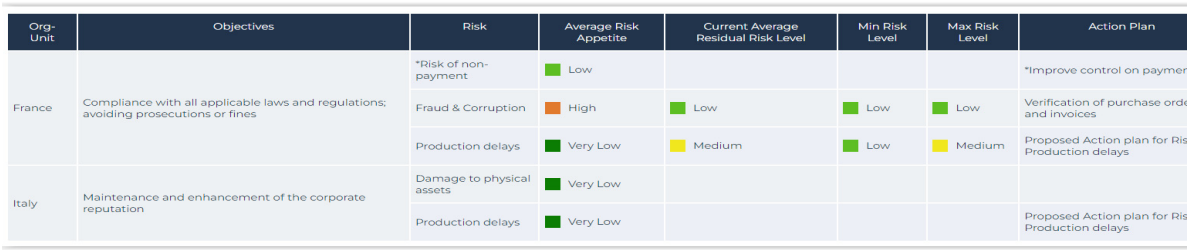
Access path

Navigation bar > Reports

Report parameters

Parameters	Parameter type	Risk selection criterion
Begin Date	Date	Not mandatory.
End date	Date	Current date by default.
Number of Entities	Entities	Not mandatory.

Report example



Org-Unit	Objectives	Risk	Average Risk Appetite	Current Average Residual Risk Level	Min Risk Level	Max Risk Level	Action Plan
France	Compliance with all applicable laws and regulations; avoiding prosecutions or fines	*Risk of non-payment	Low				*Improve control on paymer
		Fraud & Corruption	High	Low	Low	Low	Verification of purchase ord and invoices
		Production delays	Very Low	Medium	Low	Medium	Proposed Action plan for Ris Production delays
Italy	Maintenance and enhancement of the corporate reputation	Damage to physical assets	Very Low				
		Production delays	Very Low				Proposed Action plan for Ris Production delays

Aggregation Report

This report enables to sum up risk levels for an object tree (hierarchy of entities and risk types for example) as well as risk levels for each risk connected to a tree leave.

Click **Generate Aggregation** to generate aggregation data.

Access path

Navigation bar > Reports

Report parameters

This consists of defining report input data.

Parameters	Parameter type	Constraints
Begin Date	Date	Risk selection criterion. Not mandatory.
End date	Date	Risk selection criterion, fixed at current date.
Context root	The root object can be type Entity, Process or Risk Type.	Root of objects presented in rows in the report. ***Mandatory***.
Aggregation schema	Aggregation schema to be applied	***Mandatory.***
Assessed characteristics	Assessment characteristics	List of metrics presented in columns in the report. Proposed by default depending on the selected aggregation schema. ***Mandatory***.

Report example

The example below shows aggregated values of risks on entities.

Expanding an entity displays the aggregation of values on each of the risks connected to the entity.

	Avg Inherent Risk	Avg Control Level	Avg Residual Risk
MEGA Airport	Medium	Frequent observations	High
Subsidiaries	Medium	Frequent observations	High
France	High	Ineffective	High
Favoritism in selection of suppliers	High	Inexistent	High
CO2 emissions	Medium	Frequent observations	Medium
*Risk of non-payment	Medium	Frequent observations	Medium
Application Hack	Very Low	Frequent observations	Low
Fraud & Corruption	Very High	Inexistent	Very High
Natural catastrophy	High	Inexistent	High
USA	Medium	Frequent observations	Medium
Belgium	Medium	Frequent observations	Medium
Japan	High	Ineffective	High

RISK FOLLOW-UP REPORTS

Action Plan Follow-up Report

This report presents distribution of action plans on criteria such as the processes and entities concerned, process nature and status.

For more information on action plans, see Remediating Risks.

Access path

Navigation bar > Reports

Report parameters

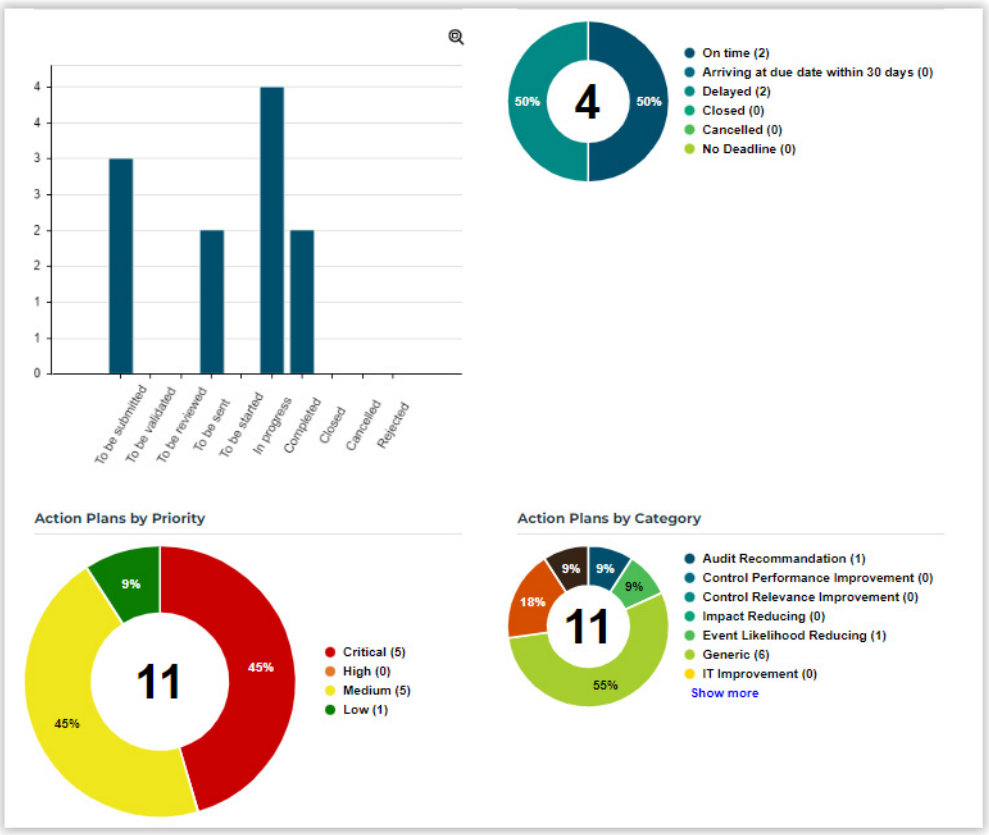
This consists of selecting action plans that will be presented in defining context elements. The action plans presented concern only those entities and processes specified in the parameters.

Parameters	Parameter type	Constraints
Begin Date	Date	Action plan selection criterion. Not mandatory.
End date	Date	Action plan selection criterion, fixed at current date.
Entities	Entity	Action plan selection criterion. Not mandatory.
Processes	Processes	Action plan selection criterion. Not mandatory.

Report example

The upper part of the report presents distribution of action plans on the following criteria:

- Distribution by nature
- Distribution by progress
- Distribution by categories
- Distribution by priorities



The lower part of the report presents distribution of action plans on the following criteria:

- Distribution by nature (corrective, Preventive)
- Distribution by process
- Distribution by entity

> ☛ *To obtain a list of risks making up a sector or a barchart bar:, click the sector (or barchart bar) that interests you.*

Session Statistics Report

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

Access path

Assessment session properties > Reports page > Statistics

Parameters

Parameters	Remarks
Campaign	Mandatory
Session	Mandatory

Report example

Respondents	5
Effective Begin Date	14/02/2022
Effective End Date	22/02/2022

	Nb Answers	% Answers
Control Level	3	100%
Very Strong	0	0%
Strong	0	0%
Medium	0	0%
Weak	1	33%
Natural catastrophy	1	33%
Very Weak	2	66%
Production delays	1	33%
Favoritism in selection of suppliers	1	33%
Likelihood	3	100%

Result

A tree appears:

- in rows: questions/answers, together with respondents

  ☛ *When expanding an answer, the risks and respondents are displayed.*

- in columns: for each question/answer, the number of respondents

This tree specifies who has answered what to which question.

RISK MANAGEMENT EFFECTIVENESS REPORTS

Risk and Incident Analysis

The Risk Manager uses this report to display:

- the risks impacting the entity for which he/she is responsible as well as its sub-entities
- The environment objects for each risk (process category and/or business line, for example)
- the mitigation status of risks managed
  - the mitigation controls
  - the incidents that determine these risks
  - the action plans concerning the risks

If, for example, the risk is gives birth to incidents, the Risk Manager can display which action plans to modify.

Path

Navigation bar > Reports

Parameters

Parameters	Constraints
Elements at risk	Mandatory

Report Content

The reports display the following in columns:

- the elements at risk (for example sites or processes)
- the associated risks
- the date of the last risk assessment
- the action plans to implement
- the action plan end date
- any incidents
- the date the incident took place

Example

Element at Risk	Risk	Last Assessed	Action Plan	Actual Completion Date	Incident	Date of Event
* Propose and sell food on the fly	*Risk of non-payment	4/24/2023	*Improve control on payments		Customer Order Processing Defect	10/15/2022
					Electricity breakdown	8/19/2022
					IT Breakdown	11/15/2022
					Operation Processing Defect	10/9/2022
	Credit card risk	2/22/2022			Credit card expired	9/22/2022
					Credit card not delivered	1/21/2022
					Credit card stolen	6/7/2022
					Falsified Credit Card	1/23/2022
					Guilty Card Payment	10/29/2022
					Major Bank Deduction Defect	8/3/2022
					Major Legal Proceedings	4/10/2021
					Major Tax penalties	2/9/2021
					Wrong credit card release	10/17/2022
					Wrong debit on professional credit card	7/25/2022

Coverage & Risks Matrix

As a Risk Manager, you must ensure the risks in your scope have associated mitigating controls. This will allow you to prioritize your control design efforts.

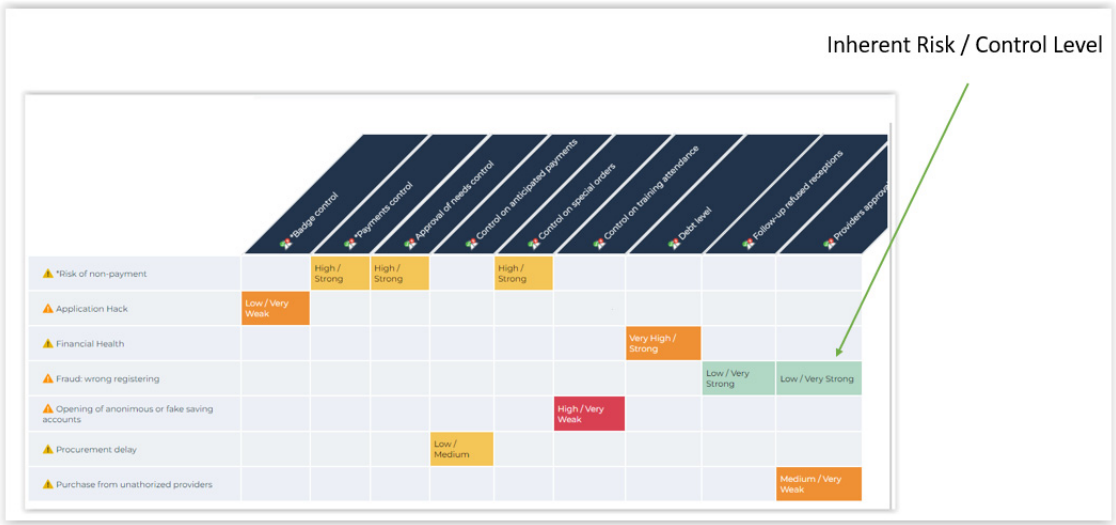
Access path

Navigation bar > Reports

Matrix content

This matrix displays:

- in rows: all the risks in the scope of the Risk Manager
- in columns: the controls whose purpose is to mitigate these risks



When a risk is mitigated by a control and an assessment has already been made, the values "Inherent risk/Control Level" are displayed at the intersection of the risk and the control. The values correspond to those obtained during the last risk assessment.

> 🕮 *The inherent (gross) risk indicates the risk to which the organization is exposed in the absence of measures taken to modify the occurrence or impact.*
>
> 🕮 *Risk control level enables characterization of control efficiency in mitigating the risk.*

Risk Trend

This report displays:

- residual risk average over the last three years
- residual risk forecast for the year to come.

Access path

Navigation bar > Reports

Report parameters

This consists in defining the context of risks presented.

Parameters	Parameter type	Constraints
Report context	risk type, entity, process, objective	Risk selection criteria presented in rows. Not mandatory.

Report example

	2021	2022	2023	Average Evolution	Action plans	Forecast 2024
Procurement delay		Low		→	No	Low
Default of payment	High	Very High		↗	No	Very High
Overdue contractual delivery date					Yes	
Invoice approved without valid justification		High		→	Yes	High
Ongoing purchase budget not under control		Medium		→	No	Medium
Favoritism in selection of suppliers		Very High	Low	↘	Yes	Very Low
Purchase not financially validated	Medium	Low		↘	No	Very Low
Supplier delivery non conforming to Purchase Order		High		→	No	High

Result computation

Computation method

Forecast Risk =

Residual Risk Year N + (Residual Risk Year N – Net Risk Year N-2)/2)

Internal values

Value name	Internal value
Very Low	1
Low	16
Medium	81
High	256
Very High	625

Example

Forecast Risk = High + ((High - Very High)/2)

Forecast Risk = 256 + ((256 – 625)/2)

Forecast Risk = 71,5 (rounded off to the nearest threshold = 81)

Forecast Risk = Medium

Hopex LDC

User Guide

Hopex Aquila

Bizzdesign

CONTENTS

Contents

COLLECTING INCIDENTS

The incident is the basic element for data collection concerning operational risk.

> 🕮 *An incident is an event occurrence, internal or external, that has an impact on the organization. It is the basic element for collection of data concerning operational risk.*

Hopex LDC (Loss Data Collection) enables you to organize follow-up of incidents and losses, to identify their causes and measure their impacts.

The system manages the complete life cycle of incidents, and you have tracking information available with a detailed history of recordings.

The GRC Manager / Incident and Loss Manager can analyze the incident before validating data. He/she can view results in the form of dynamic reports. He/she may also decide to group incidents to create a macro-incident.

- ✓ Connection Profiles to Hopex LDC
- ✓ Managing Incidents
- ✓ Specifying Incident Characteristics
- ✓ Analyzing Incidents
- ✓ Managing Macro-Incidents
- ✓ Incident Management Process

> ☛ *For more information on how to treat incidents, see the documentation concerning action plans.*

CONNECTION PROFILES TO HOPEX LDC

To connect to **Hopex**, see Logging in to Hopex.

Profiles	Desktop	Tasks
Incident and Loss Manager (Or GRC manager)	Hopex GRC	Prepares the work environment and create elements required for management of incidents and losses. Describes the environment: entities and processes, regulatory environment, IT resources Can intervene in: - declared incidents - action plans and actions
GRC Contributor	GRC Contributors	Use the simplified HOPEX Explorer desktop. - Declare incidents See The GRC Contributor Desktop.

☛ *For more details, see also Accessing the GRC Desktop.*

MANAGING INCIDENTS

Accessing incidents

To access incidents:

❱ In the navigation bar, click **Incidents**.

Filtering incidents

In the **Incidents** tab, a drop-down list enables you to view:

- **Open Incidents**

  ☛ *Open incidents are incidents that were validated by the Risk Manager.*

- **Incidents to Review**

  ☛ *The incidents to review have not been validated by the Risk Manager yet.*

- **Orphan Incidents**

  ☛ *Orphan incidents have no impact on the organization yet (they have no context object).*

  ☛ *To define the context objects impacted by an incident, open the properties of an incident and select **Characteristics > Scope > Incidents**.*

Accessing macro-incidents

To access macro incidents:

❱ Click **Incidents** and select **Macro-Incidents**.

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

  ☛ *For more details, see Managing Macro-Incidents.*

Creating incidents

To create an incident:

1. See Accessing incidents.
2. Click **New**.

   ☛ *With the "GRC Contributor" profile, click **New Incident"** from the Home Page.*

3. In the properties of the incident, enter:
   - Its **Name**
   - the **Declarant's entity**

     🕮 *An entity can be internal or external to the enterprise: an entity represents an organizational element of enterprise structure such as a management, department, or job function. It is defined at a level*

depending on the degree of detail to be provided on the organization (see org-unit type). Example: financial management, sales management, marketing department, account manager. An external entity represents an organization that exchanges flows with the enterprise, Example: customer, supplier, government office.

- the **Detection date**
- the **Occurrence Date**
- a **Description**.

☛ *For more details on these characteristics, see Specifying Incident Characteristics.*

4. Click **OK**.

SPECIFYING INCIDENT CHARACTERISTICS

To modify incident characteristics:

1. See Accessing incidents.
   The list of incidents you have declared appears in the edit area.
2. In the **Characteristics** page of the incident properties, fill in the following fields:
   - **Macro-incident**: to connect the current incident to an existing or new Macro-Incident.

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

     ☛ *For more details, see Managing Macro-Incidents.*
   - **Status**: Indicates current status of the incident in the incident management process.

     ☛ *The **Status** is grayed because it is managed automatically by the associated incident workflow. For more details, see Incident Management Process.*
   - **Declaration Date**, **Detection Date** and current **Occurrence Date**, which constitute incident key dates.

     ☛ *To specify a date, use the calendar at the right of the field.*

     ☛ *Incident declaration and detection dates can differ, the declaration date being later than the detection date.*
   - **Nature**: you may enter the nature (financial or not) of the incident.
   - **Near-miss**: check box to be selected if it is a *near-miss* incident.

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

See also: Recording Incident-Linked Amounts

RECORDING INCIDENT-LINKED AMOUNTS

When the incident has been declared, we can record amounts linked to the incident and its consequences, for example *losses*.

> 🕮 *A loss is the negative financial result of an event.*
>
> 🕮 *A gain is the positive financial consequence of an incident.*
>
> 🕮 *A provision is an amount deducted from the result to cover risks or unexpected charges. Several provisions may relate to a single risk.*
>
> 🕮 *A recovery is a sum, which in certain circumstances can reduce the amount of losses linked to operational risk. It enables recovery of a proportion of the amounts involved in the incident.*

See also: Specifying Incident Characteristics.

Accessing Incident Financial Analysis

To access financial analysis data of an incident:

1. See Accessing incidents.
   The list of incidents you have declared appears in the edit area.
2. Select the incident you wish to modify.
3. In the incident properties, select the **Financial Analysis** page.
   Total amounts appear in the **Total Amounts** section.

> ☛ *For more details on incident total amounts, see Viewing Computed Amounts Related to the Incident.*

Entering a Loss

To enter a *loss*:

> 🕮 *A loss is the negative financial result of an event.*

1. See Accessing incidents.
2. In the incident properties, select the **Financial Analysis** page.

> ☛ *For more details, see Accessing Incident Financial Analysis.*

3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Losses** tab and click the **New** button.
   The new loss appears in the list.
5. Select the new loss and click **Properties**.

6. In the **Characteristics** tab, complete the following fields:
   - **Name**
   - **Description**: comment concerning the loss.
   - **Effective Date**
   - **Nature**: "Loss of or damage to assets", "Write downs", "Loss of recourse", "Legal liability", etc.
   - **Account** in which the incident is counted.

     ☛ *For more details on the account concept, see Control Environment.*
7. Click the button next to the **Amount** field to select the loss currency.

   ☛ *Amounts entered in a currency are converted to the local currency and to the central currency.*

   ☛ *If no exchange rate has been previously defined by the administrator, the amount is automatically taken into account in the central currency.*

   ☛ *If you are not sure of the amount, you can select the **Amount is Estimated** check box. The amount entered will not be included in **Gross actual losses** related to the incident.*

   ☛ *Losses relating to a near-miss are generally estimated. It is however possible to enter actual losses.*
8. Expand the **Scope** section and, if required, enter information specific to the loss, for example:
   - **Entity** against which this loss must be accounted.

   By default, this is the same entity as that declared for the incident.
   - **Business Line** concerned by the loss.

     ☛ *For more details on elements defining scope of an incident or loss, see Defining scope of a loss.*
9. Click **OK**.

Defining scope of a loss

Scope of a loss enables definition of location of the loss, the associated incident and therefore a risk within the organization.

☛ *Organization description is detailed in chapter GRC Environment.*

The scope is specified on several component types:

- *entities* concerned by the loss

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

entity represents an organization that exchanges flows with the enterprise, Example: customer, supplier, government office.

- *business lines* concerned by the loss

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

- *risk types* to be associated with the loss

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

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

  📖 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

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

- *products* impacted by the loss

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

- *applications* impacted by the loss

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

Entering Gains

📖 *A gain is the positive financial consequence of an incident.*

To enter a gain:

1. See Accessing incidents.
2. In the incident properties, select the **Financial Analysis** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Gains** tab and click the **New** button.
   The new gain appears in the list.
5. Select the new gain and click **Properties**.
   The properties dialog box opens.
6. In the **Characteristics** tab, complete the following fields:
   - **Name**
   - **Description**: comment concerning the loss.
   - **Effective Date**
   - **Account** in which the incident is counted.

     ☛ *For more details on the account concept, see The Compliance Environment.*

7. Expand the **Amount** section and, if required, enter information concerning the loss amount.

   ☛ *Amounts entered in a currency are converted to the local currency and to the central currency.*

   ☛ *If no exchange rate has been previously defined by the administrator, the amount is automatically taken into account in the central currency.*

   ☛ *If you are not sure of the amount, you can select the **Amount is Estimated** check box. The amount entered will not be included in totals related to the incident.*

   ☛ *Losses relating to a near-miss are generally estimated. It is however possible to enter actual gains.*

8. Expand the **Scope** section and, if required, enter information specific to the gain.

   ☛ *For more details on elements defining scope of an incident, see Defining scope of a loss.*

9. Click **OK**.

Recording Recoveries

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

It is useful to differentiate between *recoveries* from insurance and those from other areas such as litigation, third-parties, etc.

To enter a recovery:

1. See Accessing incidents.
2. In the incident properties, select the **Financial Analysis** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Recoveries** tab and click the **New** button.
   The new recovery appears in the list.
5. To specify information specific to a recovery, proceed in the same way as for a gain.

   ☛ *For more details, see Entering Gains.*

Recording Provisions

📖 *A provision is an amount deducted from the result to cover risks or unexpected charges. Several provisions may relate to a single risk.*

To enter a *provision*:

1. See Accessing incidents.
2. In the incident properties, select the **Financial Analysis** page.
3. Expand the **Losses, Gains, Recoveries and Provisions** section.
4. Select the **Provision** tab and click the **New** button.
   The new provision appears in the list.

5. To specify information specific to a provision, proceed in the same way as for a gain.

☛ *For more details, see Entering Gains.*

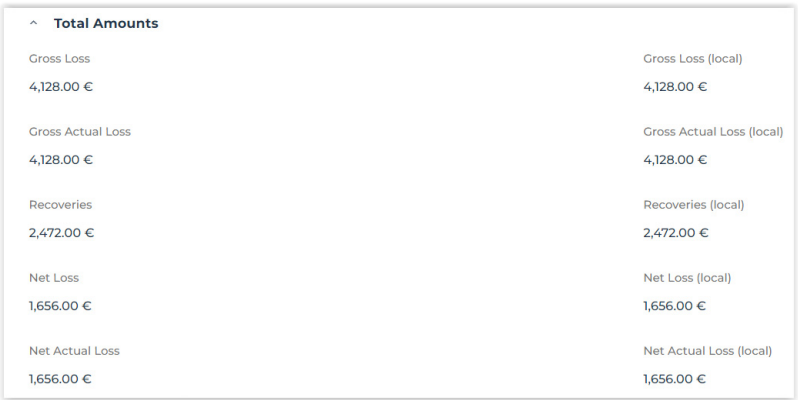
Viewing Computed Amounts Related to the Incident

To view computed amounts related to the incident:

1. See Accessing incidents.
2. In the incident properties, select the **Financial System** page.

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

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



The following fields give valuated indications on incidents:

Gross Loss

Sum of losses (including estimated losses) - Gains

Gross actual loss

Sum of losses (excluding estimated losses) - Gains

Recoveries

Sum of insurance and non-insurance recoveries

Net loss

Net Loss = Gross Loss - Recoveries

Net Actual Loss

Net Actual Loss = Gross Actual Loss - Recoveries

ANALYZING INCIDENTS

When basic characteristics of the incident have been specified, you can enter advanced characteristics in the context of incident analysis.

This work consists of linking the incident to the environment defined by your organization.

☛ *For more details on environment components, see GRC Environment.*

Incident Qualitative Analysis

To access incident qualitative analysis:

1. See Accessing incidents.
2. Open the properties of the incident.
3. In the **Characteristics** page expand the **Qualitative Analysis** section.

Risks and controls

To connect an incident to a risk and a control:

1. Click the arrow at the right of the **Materialized Risk** field and select **Connect Risk**.
2. Select the risk that interests you and click **OK**.

   🕮 *A risk is a hazard of greater or lesser probability to which an organization is exposed.*
3. Click the arrow at the right of the **Failed Control** field and select **Connect Control**.
4. Select the control that interests you and click **OK**.

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

Incident priority

To qualify the priority of an incident:

1. In the property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Specify the **Priority** characterizing the incident relative importance.
   - "High"
   - "Medium"
   - "Low"

Incident Impact

To specify the impact of an incident:

1. In the incident properties, select the **Financial Analysis** page.

2. Specify the **Impact** characterizing impact of the incident on environment elements.
   - "Very High"
   - "High"
   - "Medium"
   - "Low"
   - "Very Low"

Risk factors

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

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

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

To define risk factors associated with an incident:

1. In the property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Select the **Risk Factor** tab and click the **Connect** button.
3. Select the risk factor associated with the incident.
4. Click **OK**.

Risk consequences

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

To define risk consequences associated with an incident:

1. In the property page of an incident, select the **Characteristics** page and expand the **Qualitative Analysis** section.
2. Select the **Risk Consequence** tab and click the **Connect** button.
3. Select the risk consequences associated with the incident.
4. Click **OK**.

Incident scope

To specify the scope of an incident:

1. See Accessing incidents.
2. In the property page of Incident, select the **Characteristics** page and expand the **Scope** section.

Incident scope enables definition of risk location within the organization.

> ☛ *Organization description is detailed in paragraph Organization.*

The scope is specified on several component types:

- *entities* concerned by the incident

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

- *business lines* concerned by the incident

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

- *risk types*to be associated with the incident

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

- *process categories* and *processes* concerned by the incident

  📖 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

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

- *products* impacted by the incident

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

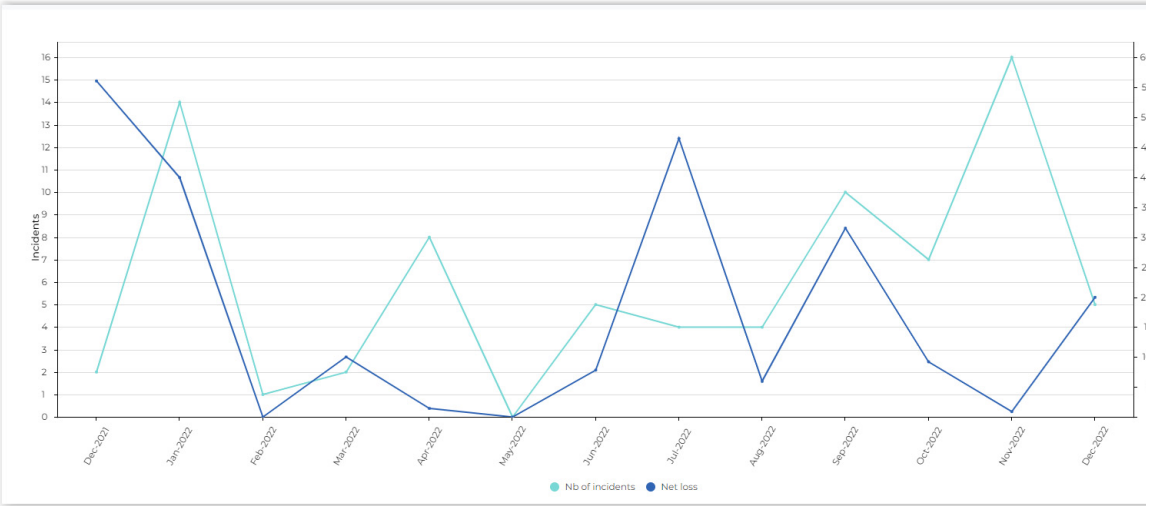
- *applications* impacted by the incident

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

Incident Impact Analysis

Hopex GRC offers the possibility to analyze, from several perspectives, the distribution of incidents linked to an element of the environment.

For more information, see Loss Analysis Reports.



MANAGING MACRO-INCIDENTS

An incident concerns only one business line and one organizational unit, which is why **Hopex GRC** enables creation of macro-incidents.

The *macro-incident* enables representation of a group of incidents that have generated losses on different business lines and/or different companies of the group.

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

For example, a willful incident in a building can have consequences on several business lines or organizational units.

Connecting Incidents to Macro-Incidents

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

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

To connect an incident to the macro-incident:

1. See Accessing incidents.
2. Select the incident you want to modify and click **Properties**.
3. Select the **Characteristics** tab.
4. Click the arrow at the right of the **Macro-Incident** field and select **Link Macro Incidents**.
5. Select the macro-incident that interests you and click **OK**.

> ☛ *Incidents are visible in the **Incidents** page of the macro-incident.*

Creating a Macro-Incident

> ☛ *This feature is proposed only to Risk Managers and Incidents and Losses Managers.*

To create a macro incident:

1. In the navigation bar, click **Incidents > Macro-Incidents**.
2. Click **New** and specify a **Name**.
3. Click **Next** and connect existing incidents.

> ☛ *For more details on elements defining scope, see Defining scope of a loss.*

Analyzing a Macro-Incident

Incidents connected to the macro-incident

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

- In macro-incident properties, select the **Incidents** page.

> ☛ *In the **Incidents** page of the macro- instance, the fields **Validated Incidents**, **First Occurrence** and **Last Occurrence** are completed automatically.*

Macro-incident amounts

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

The following fields are calculated automatically:

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

Losses evolution report

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

To access the Reports tab:

- In macro-incident properties, select the **Loss Evolution** page.

INCIDENT MANAGEMENT PROCESS

Incident Management Process General Description

Incident management process steps are as follows:

- Having specified characteristics of a new incident, the incident declarant should **Submit** the incident.
  The incident approver receives an e-mail and the new incident appears with status "Submitted".

  ☛ *To specify the incident approver, see Specifying responsibilities within an entity.*
- When an incident has been submitted by its declarant, the incident approver can **Request modifications** of the incident which takes status "Project".
  A e- mail is sent to the incident declarant.
- The Risk Manager can:
  - **Validate** the incident, which takes status "Validated".
  - **Reject** the incident.
- When a validated incident is considered as terminated, the Risk Manager can **Close** the incident, which takes status "Closed".

  ☛ *See also Incident Workflow workflow definition diagram.*

Incident Management Process Steps

☛ *To view the incident workflow definition diagram, see Incident Workflow.*

Submitting incidents

When you have specified information concerning the incident, you can submit it for approval.

To submit an incident:

1. See Accessing incidents.
2. Select the incident you want to submit and click **Workflow > Submit**.

If the entity of the incident declarant has an "Incident Approver" role, the incident takes status "To Be Approved" and appears in the list of incidents to be approved by the Incident Approver. If not, the incident status switches to "To be validated" and the incident appears in the list of incidents to be validated by the Risk Manager.

Approving incidents

After submitting the incident for approval, the incident approver of the declarant's entity can review and complete the incident and submit it for validation.

☛ *If there is no incident approver on the entity, the incident directly goes through the validation stage. See Validating incidents.*

To approve an incident:

1. Click **Incidents**.
2. Select the incident to be approved and click **Workflow**.
3. Select one of the following transitions:
   - **Approve and submit**: the incident status switches to "To be validated".
   - **Request changes**
   - **Reject**

Validating incidents

When incidents have been specified with their losses, recoveries and provisions, you can validate them.

☛ *Only Risk Managers are authorized to validate incidents.*

To validate an incident:

1. Click **Incidents**.
2. In the drop-down list, select **Incidents**
   The list if incidents for which you are responsible appears.
3. Select the incident you want to handle and click **Workflow**.
4. Select one of the following transitions:
   - **Validate** the incident status turns to "Validated"
   - **Request changes**
   - **Reject**

Closing incidents

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

☛ *Only Risk Managers are authorized to close incidents.*

To close an incident:

1. Click **Incidents**.
2. In the drop-down list select **Open incidents**.
3. Select the incident you want to submit and click **Workflow > Close**.

INCIDENT-RELATED REPORTS

The different report templates proposed as standard by **Hopex LDC** enable analysis and follow-up of incidents and their financial consequences. Reports are presented in the local currency of the user if the exchange rate between reference currency and local currency is specified. If the exchange rate is not specified, reports are presented in the reference currency.

☛ *For more details on the use of reports, see the **Hopex Common Features** guide.*

☛ *See also: Incident-Related Reports.*

✓ Loss Analysis Reports
✓ Back Testing Reports
✓ Capital Calculation Reports

☛ *For general information on reports, see:*

- *Accessing Reports*
- *Creating a Report*

LOSS ANALYSIS REPORTS

Incident and Loss Breakdown

This report displays distribution of incidents and losses selected according to different perspectives: by entity, by business line, by risk type or by process.

☛ *For more details on the procedure that enables connection of the incident or loss to an entity or process, see* *Defining scope of a loss**.*

Access path

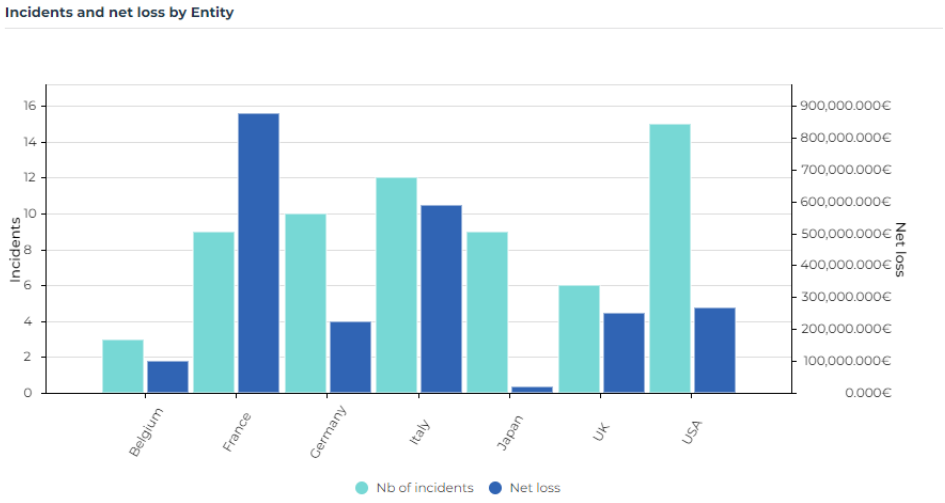
Navigation bar > Reports

Report parameters

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

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	***Risk Type***	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Process	***Process***	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Process category	***Process category***	Selection of incidents connected to process categories of the list or to sub-categories. Not mandatory.
Entities	***Entity***	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	***Business lines***	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Example



Incident and Loss Evolution by Month

This report displays monthly distribution of incidents and monthly distribution of losses on two different diagrams.

☛ *For more details on how to connect an incident to a loss, see Entering a Loss.*

Access path

Navigation bar > Reports

Report parameters

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

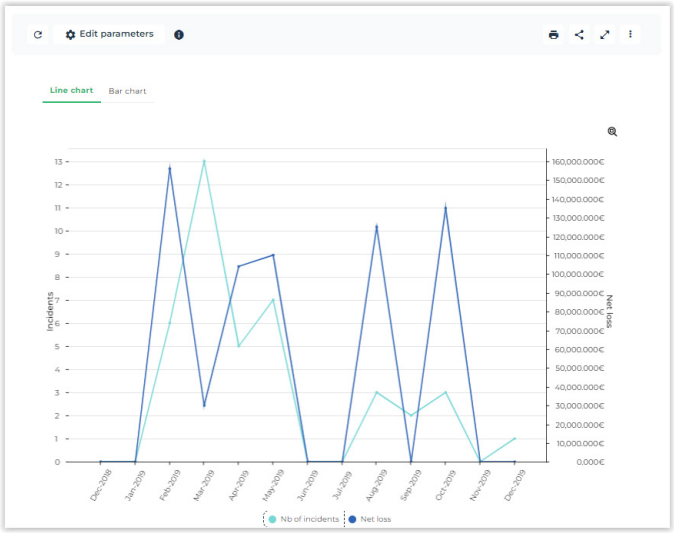
Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.

Parameters	Parameter type	Constraints
End date	Date	Current date by default.
Risk Type	Risk Type	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Process	Process	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Process category	Process category	Selection of incidents connected to process categories of the list or to their sub-categories. Not mandatory.
Entities	Entity	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	Business lines	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Results

This report displays the number of incidents and the corresponding net loss (sum of losses - sum of recoveries) per month between two dates.

☛ *If no parameter is defined, all incidents are taken into account. Otherwise, only the incidents connected to the objects specified as a parameter and their children (risk types, process categories, processes, entities and business lines) are displayed.*



Incident and Loss Evolution by Risk Type

This report displays monthly evolution curves of incidents and losses in the same diagram.

☛ *For more details on how to connect an incident to a loss, see Entering a Loss.*

Access path

Navigation bar > Reports

Report parameters

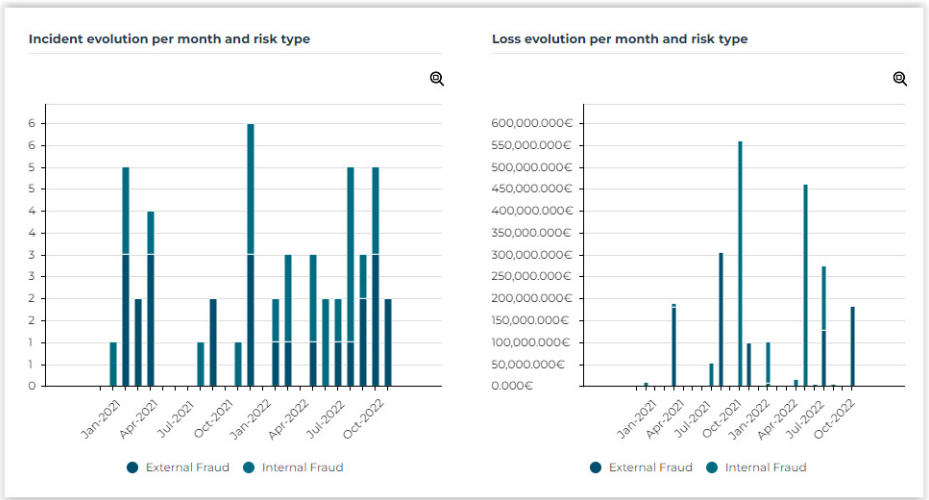
This report consists in selecting incidents and losses that will be presented while specifying the risk types in their their scope.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. The user currency is used by default.
Warning threshold	Real	Takes into account the incidents whose loss amount is higher than this threshold.
Begin Date	Date	One year before the current date (by default)
End date	Date	Current date (by default)
Risk Type	Risk Type	Selection of incidents connected to risk types of the list or to their subtypes. Not mandatory.

Results

This report consists of two parts:

- **Incident evolution** per month and risk type: displays the number of incidents declared per month between a defined start date and end date, and distributed by risk type.
- **Loss evolution** per month and risk type: displays the net loss (sum of losses - sum of recoveries) of a set of incidents.



☛ *For these two report chapters, if no risk type is defined as a parameter, all incidents are taken into account. Otherwise, only the incidents connected to the selected risk types and their children are displayed.*

BACK TESTING REPORTS

These reports indicate financial losses of risks studied from their attached incidents.

☛ *For more details on the procedure that enables connection of an incident or loss to a risk type, see Defining scope of a loss.*

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

Losses by Risk (Back Testing)

Access path

Navigation bar > Reports

Report parameters

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

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Incident net loss threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	***Risk Type***	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.
Processes	***Processes***	Selection of incidents connected to processes of list or to their sub-processes. Not mandatory.
Process category	***Process category***	Selection of incidents connected to the process categories of the list or to their sub-categories. Not mandatory.
Entities	***Entity***	Selection of incidents connected to entities of list or to their sub-entities. Not mandatory.
Business lines	***Business lines***	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Result

Risk code	Risk	Net Risk Level	Nb of incidents	Gross Loss	Gross Actual Loss	Recoveries	Net loss	Net Actual Loss
E-R14	Fraud & Corruption	Very Low	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R01	Data encryption	Low	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R02	Unauthorized spending	Medium	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
MR0374	Unprecise measurement of the procurement department	High	1	129,216.00 €	129,216.00 €	1,526.00 €	127,690.00 €	127,690.00 €
E-R23	Insufficient budget	Very Low	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
SR0543	Burried substances	High	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
P-R10	Creation of an imaginary supplier	Medium	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R18	Damage to physical assets	Medium	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R17	Credit card risk	Medium	9	1,091,944.00 €	1,091,944.00 €	62,784.00 €	1,029,160.00 €	1,029,160.00 €
CR0234	Data Retention and Disposal	High	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R07	Favoritism in selection of suppliers	Low	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R04	CO2 emissions	Medium	0	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €
E-R13	Application Hack	Low	3	486,240.00 €	486,240.00 €	77,544.00 €	408,696.00 €	408,696.00 €

Incident X Risk Level by Risk Type (Back Testing)

Access path

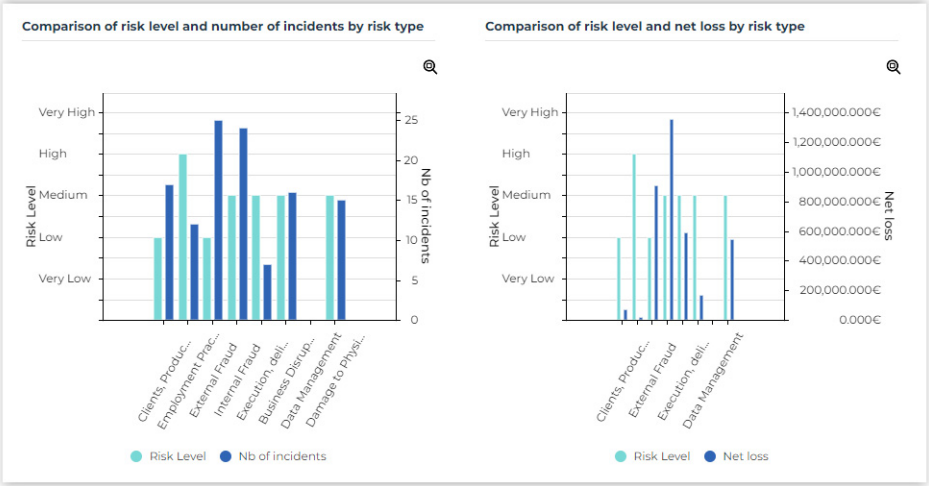
Navigation bar > Reports

Report parameters

This consists in selecting risk types that will be presented in the report.

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning threshold	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Risk Type	***Risk Type***	Selection of incidents connected to risk types of list or to their sub-risk types. Not mandatory.

Result



Incidents X Risk Level by Business Line (Back Testing)

This consists of selecting business lines that will be presented in the report.

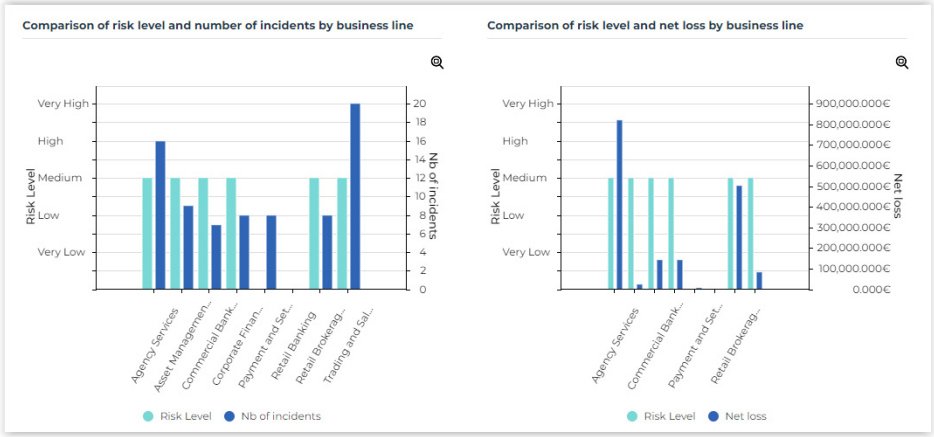
Access path

Navigation bar > Reports

Report parameters

Parameters	Parameter type	Constraints
Currency	Currency	Currency of reports. Local currency is used by default.
Warning thresh-old	Real	Minimum amount of displayed losses.
Begin Date	Date	One year before current date by default.
End date	Date	Current date by default.
Business lines	***Business lines***	Selection of incidents connected to business lines of list or to their sub-business lines. Not mandatory.

Result


Comparison of risk level and number of incidents by business line
Very High
High
Medium
Low
Very Low
Risk Level
20
18
16
14
12
10
8
6
4
2
0
Nb of incidents
Agency Services
Asset Managemen...
Commercial Bank...
Corporate Finan...
Payment and Set...
Retail Banking
Retail Brokerag...
Trading and Sal...
Risk Level
Nb of incidents
Comparison of risk level and net loss by business line
Very High
High
Medium
Low
Very Low
Risk Level
900,000,000€
800,000,000€
700,000,000€
600,000,000€
500,000,000€
400,000,000€
300,000,000€
200,000,000€
100,000,000€
0.000€
Net loss
Agency Services
Commercial Bank...
Payment and Set...
Retail Brokerag...
Risk Level
Net loss

CAPITAL CALCULATION REPORTS

These reports are used to evaluate amount of capital to be provided to cover operational risks.

Loss Distribution Matrix

This report indicates distribution of losses as a function of business lines (presented in columns) and risk types (presented in rows).

For each pair (business line, risk type), this report presents:

- The total amount of losses,
- The minimum amount of losses,
- The maximum amount of losses,
- The number of incidents.

Access path

Navigation bar > Reports

Report parameters

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

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

Report

		Airport	Banking	Industry
Business Disruption & System Failure	Total Loss	12,289.00 €	154,620.00 €	3,000.00 €
	Max Loss	12,289.00 €	56,064.00 €	3,000.00 €
	Min Loss	12,289.00 €	0.00 €	3,000.00 €
	Nb of incidents	**1**	**14**	**1**
Clients, Products & Business Practices	Total Loss	-	60,356.00 €	-
	Max Loss	-	18,872.00 €	-
	Min Loss	-	0.00 €	-
	Nb of incidents	**0**	**16**	**0**
Damage to Physical Assets	Total Loss	9,847.00 €	504,205.00 €	29,521.00 €
	Max Loss	7,967.00 €	250,000.00 €	25,433.00 €
	Min Loss	0.00 €	0.00 €	4,088.00 €
	Nb of incidents	**3**	**10**	**2**
Employment Practices & Workplace Safety	Total Loss	-	17,432.00 €	-
	Max Loss	-	4,608.00 €	-
	Min Loss	-	0.00 €	-
	Nb of incidents	**0**	**12**	**0**

Basic Indicator Approach (BIA)

This report gives an estimate of capital amount to be allocated for a business line. For each year of the period defined by parameters, the report presents:

- The total of gross revenues, by year

  ☛ *To create revenues, see Entering gross revenues for incident management.*

- The average gross revenue over the number of years specified as parameter
- The BIA defined as parameter
- The capital amount to be allocated for the business line (percentage of BIA applied to average gross revenue).

Access path

Navigation bar > Reports

Report parameters

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

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

Result

	2014	2015	2016	2017	2018	2019
Gross Income	0.00 €	66,000,000.00 €	76,000,000.00 €	67,000,000.00 €	68,000,000.00 €	-
Average Gross Income	N/A	33,000,000.00 €	71,000,000.00 €	71,500,000.00 €	67,500,000.00 €	34,000,000.00 €
BIA%	-	10%	10%	10%	10%	10%
Capital Allocation	-	3,300,000.00 €	7,100,000.00 €	7,150,000.00 €	6,750,000.00 €	3,400,000.00 €

Standardised Approach (TSA)

This report, derived from Basel II, gives an estimate of capital amount to be allocated by business line.

For each business line, the report presents:

- The total of gross revenues, by year
- The average gross revenue over the number of years specified as parameter
- The TSA rate adopted for the business line
- The capital amount to be allocated for the business line (percentage of TSA applied to average gross revenue).

Access path

Navigation bar > Reports

Report parameters

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

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

Result

	TSA%	Item	2015	2016	2017	2018	2019
Agency Services	13.0%	Gross Income	0.00 €	0.00 €	0.00 €	0.00 €	-
		Average Gross Income	N/A	0.00 €	0.00 €	0.00 €	0.00 €
		TSA%	-	13.0%	13.0%	13.0%	13.0%
		Capital Allocation	-	0.00 €	0.00 €	0.00 €	0.00 €
Asset Management	11.0%	Gross Income	0.00 €	0.00 €	0.00 €	0.00 €	-
		Average Gross Income	N/A	0.00 €	0.00 €	0.00 €	0.00 €
		TSA%	-	11.0%	11.0%	11.0%	11.0%
		Capital Allocation	-	0.00 €	0.00 €	0.00 €	0.00 €
Banking	12.0%	Gross Income	66,000,000.00 €	76,000,000.00 €	67,000,000.00 €	68,000,000.00 €	-
		Average Gross Income	N/A	71,000,000.00 €	71,500,000.00 €	67,500,000.00 €	34,000,000.00 €
		TSA%	-	12.0%	12.0%	12.0%	12.0%
		Capital Allocation	-	8,520,000.00 €	8,580,000.00 €	8,100,000.00 €	4,080,000.00 €
Commercial Banking	15.0%	Gross Income	0.00 €	0.00 €	0.00 €	0.00 €	-
		Average Gross Income	N/A	0.00 €	0.00 €	0.00 €	0.00 €
		TSA%	-	15.0%	15.0%	15.0%	15.0%
		Capital Allocation	-	0.00 €	0.00 €	0.00 €	0.00 €

Hopex Cyber Resilience

User Guide

Hopex Aquila

Bizzdesign

CONTENTS

Contents

Introduction to Hopex Cyber Resilience

See also:

- Steps in the Cyber Resilience Process
- ICT Vendors
- ICT Risks
- Cyber Resilience Reports

Definition of Cyber Resilience

Cyber resilience is the ability for an entity to ensure its integrity and implement preventive actions against cyber attacks. It is a global approach which encompasses both cybersecurity and Business Continuity Management.

Context

Hopex Cyber Resilience enables you to initiate and implement resilience strategies, ensuring continuity for your business operations. It enables compliance with a variety of local regulations, focusing on ICT risk assessment and cyber resilience standards, such as:

- DORA (EU): applicable as from January 2025 to all companies operating in the European Union.
- CSF (NIST, USA)
- PRA Operational Resilience (BoE, UK)
- Sound Practices to Strengthen Operational Resilience (OCC, USA)
- CPS 234 (APRA, Australia)
- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI, India)

Use together with other solutions

Hopex Cyber Resilience can be used together with:

- **Hopex BCM**
- **Hopex GRC**
- **Hopex IT Portfolio Management**

> ☛ *You can also use the UCF regulatory framework to speed up your cyber compliance initiative (see About Unified Compliance Framework).*

Installation of the Cyber Resilience (CYRES) Module

Prerequisites:

You must have first installed the "ITPM Excel Import Template" module.

> ☛ *For more details on module installation, see Importing a Module into HOPEX.*

BUILDING CYBER RESILIENCE

- ✓ Steps in the Cyber Resilience Process
- ✓ ICT Vendors
- ✓ ICT Risks
- ✓ Cyber Resilience Reports

STEPS IN THE CYBER RESILIENCE PROCESS

Hopex Cyber Resilience is a module which can be used throughout your cyber resilience initiative.

See also:

- Introduction to Hopex Cyber Resilience
- ICT Vendors
- ICT Risks
- Cyber Resilience Reports

Managing the ICT Environment

Objec types managed by the GRC solutions

GRC solutions enable to manage:

- enterprise processes

  ☛ *See Managing Process Categories and Processes.*

- associated IT resources

  ☛ *See Managing Applications.*

- ICT-related risks

  ☛ *See Managing Risks.*

Object types managed by Hopex Cyber Resilience

Hopex Cyber Resilience enables to view the followed object types:

- Technology

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

  *To manage technologies, go to **Environment > Organization > Technologies**.*

- Data center

  🕮 *A data center is a physical site that groups together IT facilities responsible for storing and distributing data through an internal network or via Internet access.*

- Facility

  🕮 *A facility is a model of site of interest for the enterprise (for example: factory, outlet).*

- Server (deployed)

  🕮 *A (deployed) server is a computer on which applications are run.*

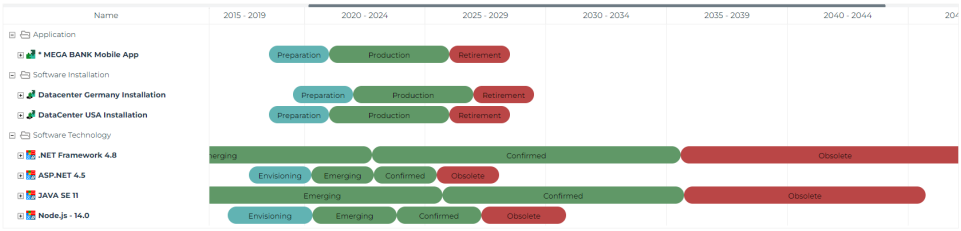
- Data Category

  🕮 *A data category represents a type of data with shared characteristics (for example: sensitive data, confidential data).*

You can view ***Business Impact Analysis*** and ***Business Continuity Plans*** in the properties of the following object types:

- technologies
- data centers
- facilities
- servers (deployed)

You can view a ***Gantt diagram*** in the properties of applications and software technologies:



MS Excel to build the resilience environment

An Excel template enables to speed up the creation of objects which are necessary to implement a cyber resilience initiative.

For more details on Excel Models, see the Common Features documentation on Excel.

Modules complementary to Hopex Cyber Resilience

The **Hopex Cyber Resilience** module can be used together with :

- ITPM Discovery, to provide automated discovery of an organization's on-premises technologies and applications.
  - ☛ *See Inventorying Technologies with ITMC Discovery.*
- **AI-Driven APM** (Ai-driven APM), to distinguish technologies from business applications.
  - ☛ *See Distinguishing Applications from Technologies.*
- **ServiceNow Integration**, to synchronize objects between **Hopex** and ServiceNow.
  - ☛ *See ServiceNow Integration.*

Identifying Critical IT Processes and Resources

You need to identify risks related to Information and Communication Technologies (ICT).

You must perform BIAs to identify critical processes and critical assets.

☛ *See Defining a Business Impact Analysis.*

The **BIA Impacts** report is a dendrogram which displays risks, applications, and technologies. You may click the elements of the dendrogram to expand the report.

When you hover the mouse over an object, a tooltip might display information about the object, when available.

☛ *This report is available in the **Reports** page of BIA properties (**Continuity > Business impact Analysis**).*

Assessing the Cyber Resilience Framework

Cyber-related risks must be assessed. A specific questionnaire template is available.

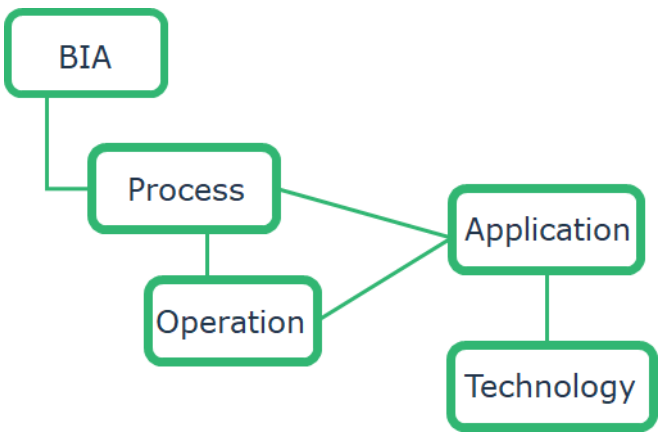
☛ *See ICT Risks.*

Planning the Cyber Resilience Initiative

You must document and test Business Continuity Plans.

☛ *See Designing a Business Continuity Plan and Testing a Business Continuity Plan.*

You can view BIAs and BCPs in the properties of applications and software technologies linked to critical processes.



Managing Cyber-Related Incidents

You must document, notify, and follow-up cyber incidents.

☛ *For general information on incidents, see Collecting Incidents .*

Incident causes and incident type

In the incident properties, select the **Qualitative Analysis** section enables to:

- Enter the incident **Root Cause Description**.
- Select the **Incident type**.

📖 *The Incident type corresponds to the materialized risk type.*

Major incident

An incident may be considered as **Major**  (check box in the Incident properties **Characteristics** page.

📖 *An incident is considered as major when it has a high and adverse impact on important or critical organization functions.*

This is a useful characteristic when it comes to generating the Major Incidents MS Word report. See Major Incident Report (MS-Word).

Calculation of time elapsed since the incident detection

A computed characteristic enables to display the number of days/hours elapsed since the detection of the incident.

This computed characteristic is displayed:

- in the **Characteristics** page of the incident properties
- in column, in the list of incidents accessible from the **Incidents** menu
- in the Major Incident MS Word report
- in the **Incidents** properties of the following object types:
  - risks
  - process categories
  - processes
  - macro-incidents
  - Org-Units
  - applications
  - business lines
  - products

Reports Related to Incidents

Specific reports allow you to:

- generate a Major incident reports to inform authorities.

  ☛ *See Major Incident Report (MS-Word).*

- analyze incidents.

  ☛ *See Incident Bow-Tie Analysis.*

- monitor cyber-related incidents.

  ☛ *See Incident Monitoring.*

Viewing the BCPs triggered after a incident

In an incident properties, the **Crisis Management** page gives you indications on the triggered BCPs.

☛ *This page is available if at least one triggered BCP is connected to the incident.*

Monitoring Cyber Resilience

Reports enable you to monitor your cyber resilience initiative.

For more details, see Cyber Resilience Reports.

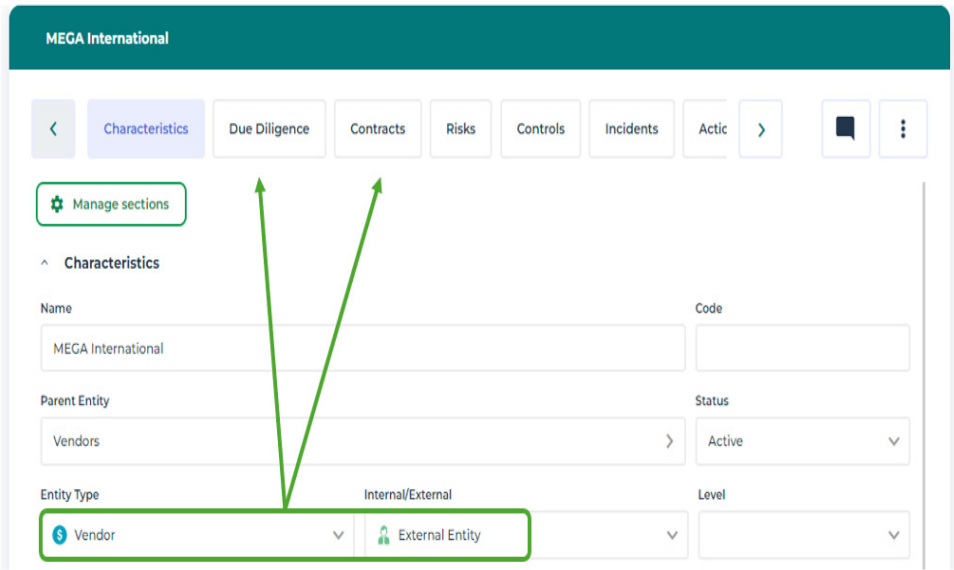
ICT VENDORS

An ICT vendor is a company which provides ICT services (Information and Communication Technologies).

In **Hopex** a vendor is an ***external*** org-unit of ***Vendor*** type.

When en entity is an ***external*** org-unit of ***Vendor*** type, you can:

- perform due diligence on the vendor
- specify the contracts with this vendor



Listing ICT Vendors

To list ICT vendors:

1. In the navigation bar, select **Environment > Organization > Vendors**.

   ☛ *The hierarchy of vendors is also available from **Processes > By entity > Vendors**.*

   The "Vendors" folder is available if there is at least one vendor in the repository.

Creating an ICT Vendor

To create an ICT vendor:

1. See Listing ICT Vendors.
2. Click **New**.
   The vendor is automatically created.

   ☛ *You may notice from the vendor properties that it is an org-unit of Vendor type.*

Specifying Vendor Contracts

Listing contracts

To list contracts:

- In the navigation bar, select **Environment > Organization > Vendors and Contracts**.
  You may, through specific lists, list:
  - all **Contracts**
  - **Contracts by Vendor**

To list the contracts of an ICT vendor:

1. In the navigation bar, select **Environment > Organization > Vendors and ContractsContracts by vendor**.
2. In a vendor properties, select the **Contracts** page.

Creating a contract

To create a contract:

1. In the navigation bar, select **Environment > Organization > Vendors and Contracts> Contracts**.
2. Click **New**.
3. (Optional) Enter:
   - the **Begin Date**
   - the **End date**
   - the **Code**
   - **Contract type**
   - a **Vendor**
4. Click **OK**.

Viewing the contract status

Once the contract has been created, the **Status** is automatically assigned:

- **Signed**

  ☛ *The contract is considered "signed" when today's date is less than the contract begin date.*

- **Live**

  ☛ *The contract is considered "ongoing" if today's date is within the date range between the contract begin date and end date.*

- **Expired**

  ☛ *The contract is considered "Expired" when today's date is greater than the contract end date.*

- **Unknown**

  ☛ *The status is unknown when dates are not specified.*

Specifying the contract characteristics

In the properties of a contract you may specify the following:

- **Contract Type**
- **Vendor** concerned by the contract
- **Signatory** entity
- **Contract Elements**
  You may connect the objects which are part of the contract:
  - Application

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

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

    📖 *A process describes how to implement all or part of the process required to make a product or handle a flow.*
  - Operation

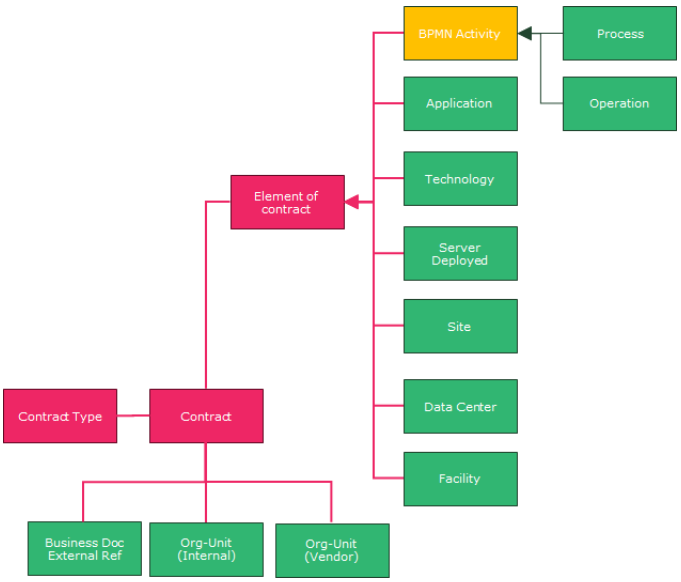
    📖 *An operation is an elementary step in a process. It corresponds to the intervention of an entity withing the organization.*
  - Server

    📖 *A (deployed) server is a computer on which applications are run.*
  - Site

    📖 *A site is a geographical location of an enterprise. Examples: Boston subsidiary, Seattle plant, and more generally the headquarters, subsidiaries, plants, warehouses, etc.*
  - Data center

    📖 *A data center is a physical site that groups together IT facilities responsible for storing and distributing data through an internal network or via Internet access.*
  - Installation

    📖 *A facility is a model of site of interest for the enterprise (for example: factory, outlet).*



Attachments

In the **Attachments** section you can attach the actual contract.

For more information on business documents see Using Business Documents.

Assessing ICT Vendors

Assessing an ICT Vendor

To assess an ICT vendor:

1. In the properties of a vendor, select the **Due Diligence** page.
2. Click **New Assessment**.
3. (Optional) Edit the **Date**.
4. Specify whether the vendor is:
   - **Compliant**

     ☛ *A vendor who is considered "Compliant" is compliant with the cybersecurity requirements. He can be considered as reliable and secure and may be a preferred partner for collaboration.*
   - **Potential**

     ☛ *A vendor who is considered "Potential" has passed the cyber due diligence but may require improvements or additional monitoring to fully meet the cybersecurity requirements. He may be seen as a promising partner but might need further effort to enhance cybersecurity.*
   - **Critical**

     ☛ *A vendor who is considered "Critical" has significant cybersecurity risks or vulnerabilities. He can be acceptable for certain types of services or collaborations with appropriate mitigation measures.*

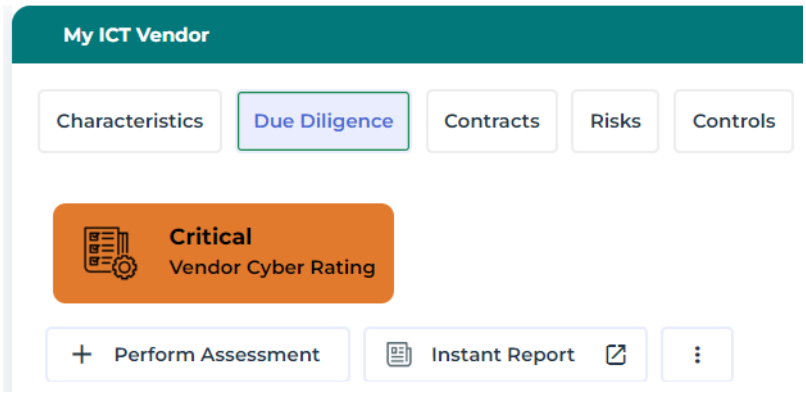
However, he requires special monitoring and attention due to the associated risks.

- **Non-Compliant**

  ☛ *A vendor who is considered "Non-compliant" fails to meet the minimal cybersecurity requirements and pose high risks to data and operations security. It may be necessary to avoid or terminate collaboration with him due to a high risk of non-compliance and potential compromise to the overall security of the organization.*

5. Click **OK**.
   The vendor rating appears. All the assessments appear in the form of a list.

The last **Vendor cyber rating** is displayed at the top of the page.



Assessing multiple ICT vendors

To assess simultaneously several ICT vendors:

1. In the navigation bar, click **Assessment > Direct Assessment > Multiple Due Diligence**.
2. Click **New Assessment**.
3. Select a vendor in the tree that appears and click **OK**.
4. Click each vendor (context) ans assess the **Vendor Cyber Rating**.
5. Click **Submit**.

Assessing ICT vendors via campaigns

You may assess ICT vendors via campaigns.

A "Due Diligence" assessment template is available.

To launch an assessment campaign, see Starting an Assessment Campaign.

ICT RISKS

Hopex Cyber Resilience enables to launch risk assessment on ICT assets within a defined scope.

☛ *For an overview of the risk assessment feature, see:*

- *Assessing Risks*
- *Assessment Campaigns*

This section is about ICT risk assessment specificities.

ICT Risk Assessment Template

Contexts

Hopex Cyber Resilience provides an ICT risk assessment template in the context of the following objects:

- Entity

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

- Process category

  📖 *A process category regroups several processes. It serves as a categorization level and provides access to finer grained processes.*

- Process

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

- Operation

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

  ☛ *Risks on processes and operations are retrieved only if the processes and operations are connected to a live contract.*

- Site

  ☛ *A site is a geographical location of an enterprise. Examples: Boston subsidiary, Seattle plant, and more generally the headquarters, subsidiaries, plants, warehouses, etc.*

- Application

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

- Software technology

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

- Deployed server

  📖 *A (deployed) server is a computer on which applications are run.*

- Data center

  📖 *A data center is a physical site that groups together IT facilities responsible for storing and distributing data through an internal network or via Internet access.*

- Installation

  📖 *A facility is a model of site of interest for the enterprise (for example: factory, outlet).*

- Contract

  📖 *A contract is a written agreement between the organization and a vendor.*

- Vendor

  ☛ *A vendor is a external org-unit of "Vendor" type.*

Respondents

Respondents are defined as follows:

Context object type	Responsibility (business role)
Technology	Local Technology Correspondent
Application	Local application owner, IT owner
Processes	Risk assessor
Process category	Risk assessor
Entity / Vendor	Risk assessor, Risk Manager

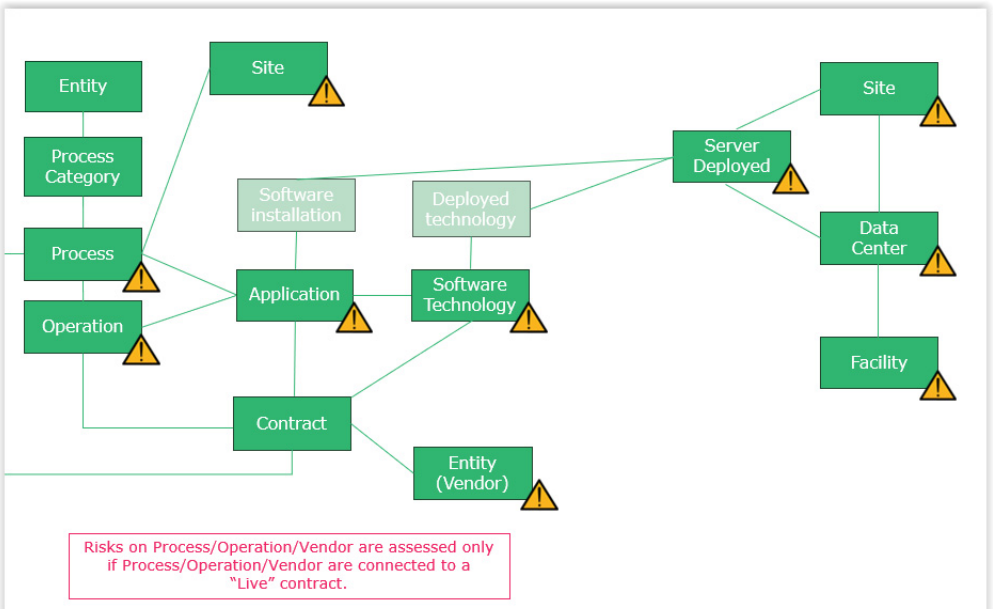
Questionnaire rendering

The questionnaire is in the form of a heatmap.

☛ *For more details, see Using Heatmap Questionnaires.*

Prerequisites to ICT Risk Assessment

To assess ICT vendors, you must have first connected the objects of your environment in an appropriate way.



Launching an ICT Risk Assessment

You can assess several risks simultaneously via an ***interactive heatmap***.

To assess several cyber-related risks simultaneously:

1. In the navigation bar, click **Assessment > Direct Assessment > Risk Multiple Assessment**.
2. Click **New Assessment**.
3. In the window that appears, select the **ICT Risk Assessment Assessment template**:
4. In the displayed tree, select the entity that defines the assessment context.
5. Expand the tree to find the relevant processes and applications.

   ☛ *A risk is assessed in the context of elements of the branch from the risk up to the root.*
6. For the rest of the procedure, see Assessing Multiple Risks Simultaneously .

   ☛ *ICT risks can also be assessed through assessment campaigns. See Assessment Campaigns for further information.*

CYBER RESILIENCE REPORTS

- ✓ ICT Service Providers and Contracts
- ✓ Gantt of ICT Service Provider Contracts
- ✓ Vendors' Contracts (MS Word) Report
- ✓ Incident Monitoring
- ✓ Incident Impacts
- ✓ Major Incident Report (MS-Word)
- ✓ Incident Bow-Tie Analysis
- ✓ Process Impacts
- ✓ Process ICT Impacts Overview
- ✓ Risk Dashboard by Risk Type
- ✓ Process Criticality and Supporting ICT Assets Table Overview
- ✓ Vendors Overview by Process
- ✓ Critical ICT Assets (from Process/Entity)

ICT Service Providers and Contracts

This report gives an overview of the contracts signed with ICT vendors in a specific period of time.

☛ *For more details, see ICT Vendors.*

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. (Optional) Use filters to find the **ICT Service Providers and Contracts** report.

Illustration

Table / Matrix

Report parameters

Parameters
Begin Date
End date

Report Content

This report is displayed in the form of a table and contains the following columns:

- Contract name
- Vendor
- Cyber rating

☛ *See Specifying Vendor Contracts.*

- Contract type
- Code
- Resource
- Resource type
- Begin Date
- End date
- Status
- Attachments
- First year (yes/no)

☛ *Vendors whose contract was signed less than a year ago need to be closely monitored.*

Report example

Contract Name	Vendor	Cyber Rating	Contract Type	Code	Resource	Type of resource	Begin Date	End Date	Status	Attachments	First year
Amazon contract 1	My ICT Vendor	Critical		Ctr1	Server-side encryption with Amazon S3 Key Management Service	Software Technology	12/1/2023	4/24/2024	Live	0	No
Amazon contract 2	My ICT Vendor	Critical		Ctr2	Amazon.com AWS Agent	Software Technology	3/1/2024	4/24/2024	Live	1	Yes
Microsoft contract 1	My ICT Vendor	Critical		Ctr3	Microsoft .NET Framework Win	Software Technology	4/1/2023	3/1/2024	Expired	1	No

GANTT OF ICT SERVICE PROVIDER CONTRACTS

This report consists of a Gantt chart showing the contracts signed with ICT vendors in a specific time frame.

It displays the contract lifecycle, by vendor.

☛ *For more details, see ICT Vendors.*

Path

You may generate this report:

- individually, in the **Contracts** page of a vendor properties (external org-unit of "vendor" type).
- globally, for several vendors (from the navigation bar **Reports** menu).

Illustration

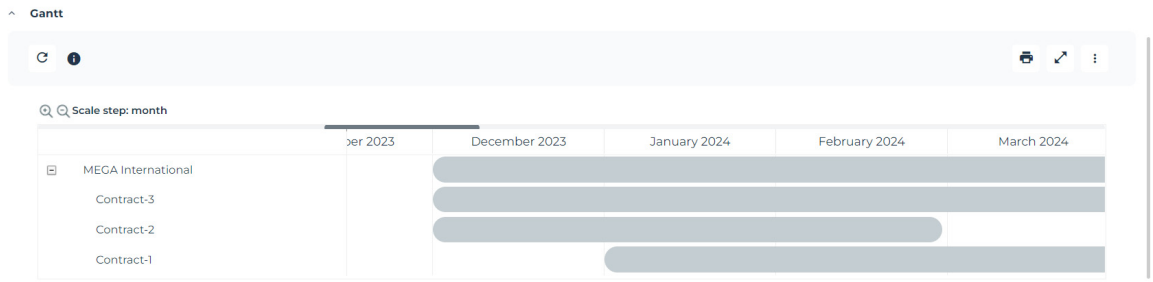
Gantt Chart

Report parameters

When you generate this report from the navigation bar **Reports** menu, the following parameters are available:

Parameters	Possible values
Contract begin date	
Contract end date	
Vendors	
Vendor cyber rating	Compliant, Potential, Critical, Non-Compliant
Contract type	

Report example



VENDORS' CONTRACTS (MS WORD) REPORT

You may generate an MS Word report that sums up the information regarding vendors and contracts.

Path

The Vendors' Contracts (MS Word) Report can be created:

- From a vendor
- From a list of vendors

To generate the report from a list of vendors:

1. See Listing ICT Vendors.
2. Select one or several vendors.
3. Click ⋮ and select **Documentation > Vendors' Contracts Report**. The report is being generated.

Illustration

MS Word report

Report parameters

The two dates to specify as a parameter enable to define a time period during which contracts start.

Vendors	
Earliest contract begin date	Includes contracts beginning on this date
Latest contract begin date	Includes contracts beginning on this date (at the latest)

Report Content

The report contains the following basic information:

- Vendor name
- Code
- Contacts (name and e-mail)
- Vendor cyber rating

It contains more detailed information on each vendor, such as:

- Last cyber due diligence
- List of contracts and elements of contracts

INCIDENT MONITORING

This report is displayed in the form of a table and details the selected incidents.

☛ *For general information on incidents, see Collecting Incidents .*

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. User filters to find the **Incident the report Monitoring** report.

Illustration

Table / Matrix

Report parameter

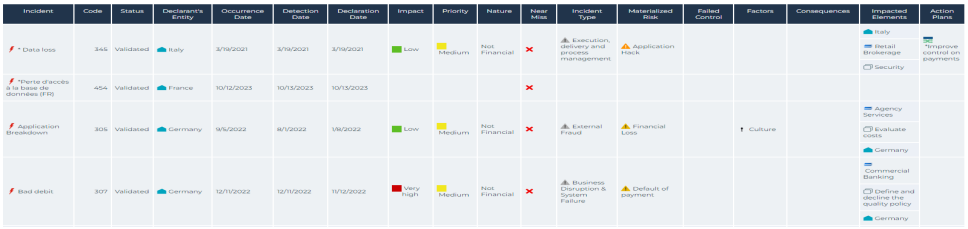
Parameter
Incident list

Report Content

This report is displayed in the form of a table and contains the following columns:

- Name
- Code
- Status
- Declarant’s entity
- Occurrence date
- Detection date
- Declaration date
- Impact
- Priority
- Type
- Near-miss
- Materialized Risk
- Failed control
- Factors
- Risk consequences
- Impacted elements
- Action plans

Report example



Incident	Code	Status	Declarant's Entity	Occurrence Date	Detection Date	Declaration Date	Impact	Priority	Nature	Near Miss	Incident Type	Materialized Risk	Failed Control	Factors	Consequences	Impacted Elements	Action Plans
* Data loss	345	Validated	Italy	3/19/2021	3/19/2021	3/19/2021	Low	Medium	Not Financial	✕	Execution, delivery and process management	Application Hack				Italy Retail Brokerage Security	*Improve control on payments
*Perte d'accès à la base de données (FR)	454	Validated	France	10/12/2023	10/13/2023	10/13/2023				✕							
Application Breakdown	305	Validated	Germany	9/5/2022	8/1/2022	1/8/2022	Low	Medium	Not Financial	✕	External Fraud	Financial Loss		Culture		Agency Services Evaluate costs Germany	
Bad debit	307	Validated	Germany	12/11/2022	12/11/2022	11/12/2022	Very High	Medium	Not Financial	✕	Business Disruption & System Failure	Default of payment				Commercial Banking Define and decline the quality policy Germany	

INCIDENT IMPACTS

This report is displayed in the form of a dendrogram illustrating the impacts of an incident.

☛ *For general information on incidents, see Collecting Incidents .*

Path

To access this report:

1. In the navigation bar, select **Incidents**.
2. Open the incident properties and in the **Reporting** page, select **Incident Impacts**.

Illustration

Dendrogram

Report parameter

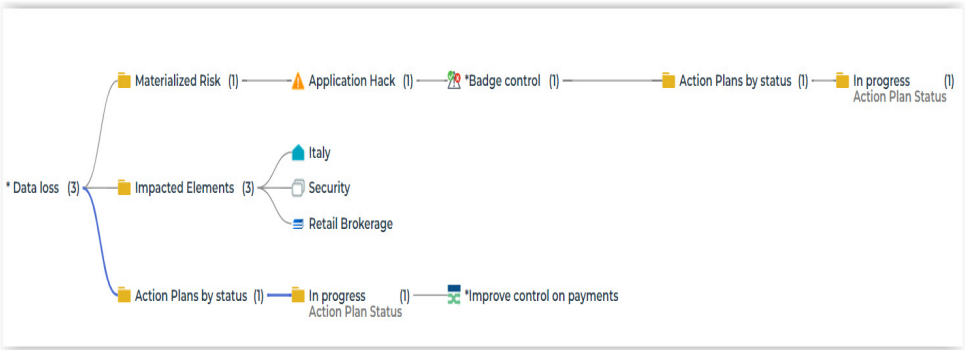
Parameter
1 Incident

Report Content

This report indicates:

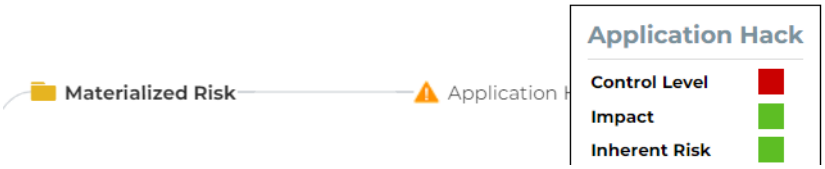
- **Action plans**, by status and priority
- the **Causal analysis** (risk factors and consequences)
- The **Materialized risk**, with:
  - information on the last assessments
  - controls connected to the risk
  - action plans by status and priority
- the **Failed control**, together with:
  - information on the last assessments (last control level)
  - action plans by status and priority
- **Impacted elements**
  - Entity
  - Process category
  - Processes
  - Application
  - Technology
  - Server
  - Site
  - Data center
  - Facility
  - Business line
  - Product

Report example



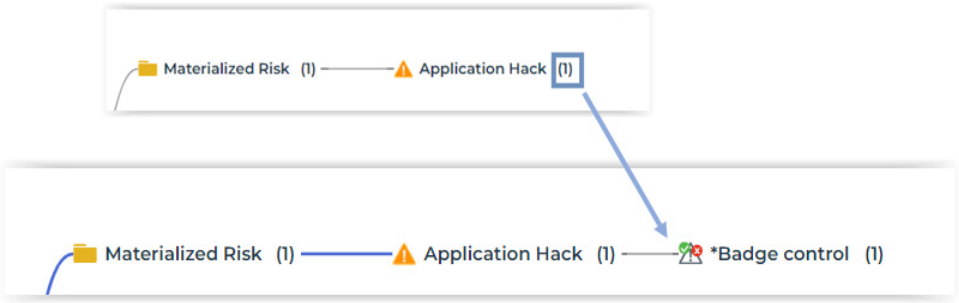
To view information about an impacted element:

- Hover the mouse over this element to display a tooltip.



To display elements in a branch:

- Click the number which is displayed next to an item.
  The tree expands.



MAJOR INCIDENT REPORT (MS-WORD)

An MS Word document enables to declare incidents to supervisory authorities.

☛ *For general information on incidents, see Collecting Incidents .*

Path

The MS-Word Major incident report can be created:

- from an incident
- from a list of incidents

To generate the major incident report from a list of incidents:

1. In the navigation bar, select **Incidents**.
2. Select the incidents to include to the report.
3. Click ⋮ then select **Documentation > Major incident report**.

Illustration

MS Word report

Report Content

The Major incident report contains the following:

Basic information on the incident

- **Code - name**
- **Major** incident (Yes/No)
- **Entity**
- **Detection date**
- **Priority**
- **Impact**
- Number of **BCPs** (Business Continuity (Plan)

Detailed information

- **Major** incident (Yes/No)
- **Priority**
- **Impact**
- **Status**
- **Occurrence date**
- **Declaration date**
- **Detection date**
- **Incident Declarant**
- **Declarant's entity**

Root Cause Analysis

- **Incident type** (risk type)
- **Materialized Risk**
- **Failed control**

Impacted elements

- **Entity**
- **Process category**
- **Processes**
- **Application**
- **Technology**
- **Server**
- **Site**
- **Data center**
- **Installation**
- **Business line**
- **Product**

Financial assertion

- **Actual gross loss**
- **Recoveries**
- **Net loss**
- **Actual net loss**

Triggered BCPs

- **Name**
- **Status**
- **Begin Date**
- **End date**
- **Result**

INCIDENT BOW-TIE ANALYSIS

This bow-tie analysis enables to visually display incident causes and consequences.

- causes (risk factors)

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

- consequences

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

Path

To access this report:

1. In the navigation bar, select **Incidents**.
2. Open the incident properties and in the **Reporting** page, select **Bow-Tie Analysis**.

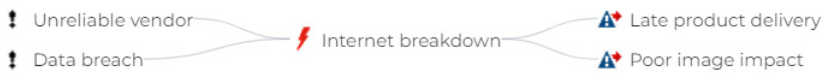
Illustration

Bow-Tie Analysis

Report parameter

Parameter
1 Incident

Report example



PROCESS IMPACTS

This report displays an overview of a process and its constituting elements, for example:

- processes
- operations
- applications
- technologies
- risks
- controls
- incidents
- Action Plans
- sites
- servers (deployed)
- data centers
- facilities

Path

To access this report:

1. In the navigation bar, select **Processes**.
2. Expand the hierarchy of process categories/processes and open the process properties.
3. In the **Reporting** page of a process, select **Reports > Process impacts**.

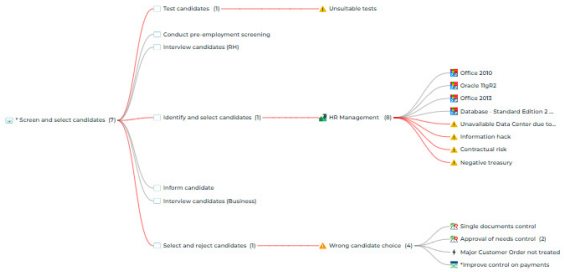
Illustration

Bow-Tie Analysis

Report parameter

Parameter
1 Process

Report example



To view information about an impacted element:

- Hover the mouse over this element to display a tooltip.

To display elements of a branch:

- Click the number which is displayed next to an item.
  The tree expands.

  ☛ *A red link indicates that there are risks in the branch.*

PROCESS ICT IMPACTS OVERVIEW

Path

Navigation bar > Reports

Illustration

Table

Report parameter

Parameter
List of processes

Report Content

This table is displayed in the form of a table of the selected processes impact analysis.

Table Columns

Column	Filter	Comment
Processes	X	
ICT resource type	X	
ICT resource	X	
Risk		Risk connected to the ICT resource

Column	Filter	Comment
Residual risk	X	
Risk action plan		
Risk action plan status	X	
Risk action plan priority	X	Action plan connected to the risk
Control		
Control level		
Control action plan		
Control action plan status	X	
Control action plan priority	X	

Report example

Process	ICT Resource Type	ICT Resource	Risk	Residual Risk	Risk Action Plan	Risk Action Plan Status	Risk Action Plan Priority	Control	Control Level	Control Action Plan	Control Action Plan Status	Control Action Plan Priority
* Screen and select candidates	Application	HOPEX	*Risk of non-payment	Medium	*Improve control on payments	In progress	Critical	*Payments control	Pass	*Improve control on payments	In progress	Critical
								Approval of needs control	Pass	*Improve control on payments	In progress	Critical
										Annual review of accounts	In progress	Critical
								Control on special orders	Pass	*Improve control on payments	In progress	Critical
			*Wrong entries of supplier contract parameters	Medium	Annual Review of supplier contracts	In progress	Critical	*Payments control	Pass	*Improve control on payments	In progress	Critical
			Application Hack	Low				*Badge control	Pass	*Improve control on payments	In progress	Critical
			Bad Technology Choices	Medium				*Badge control	Pass	*Improve control on payments	In progress	Critical
			Contractual risk	Very Low								
			Information hack	High								

Risk Dashboard by Risk Type

This report is displayed in the form of a dashboard presenting risks, controls, and incidents connected to a risk type. Several types of illustrations are available within this report.

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. (Optional) Use filters to find the **Risk Dashboard by Risk Type** report.

Illustrations

This dashboard consists of several illustration types:

- Pie charts
- Heatmaps
- Line chart

Report parameter

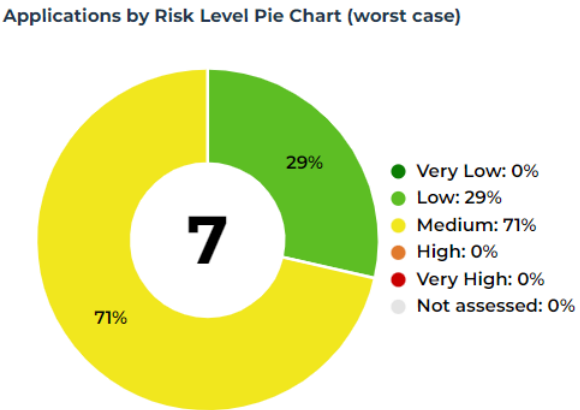
Parameter
Risk Type

Dashboard Content

Residual risk level

Pie charts display the level of residual risk for several object types (worst case scenario):

- Processes
- Applications
- Technologies
- Vendors
- Sites
- Servers (deployed)
- Facilities
- Data centers

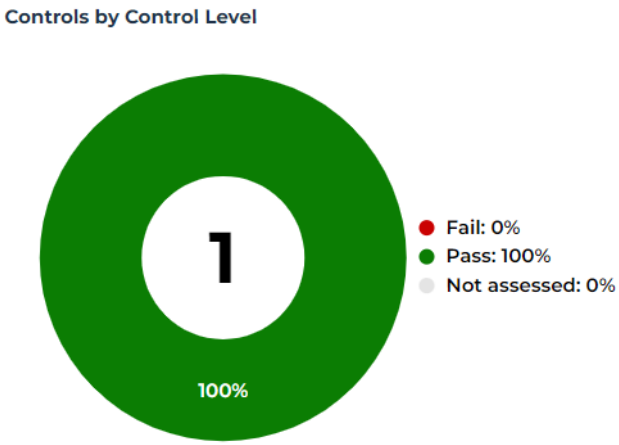


In the above example, 71% of the processes have a "Medium" risk level.

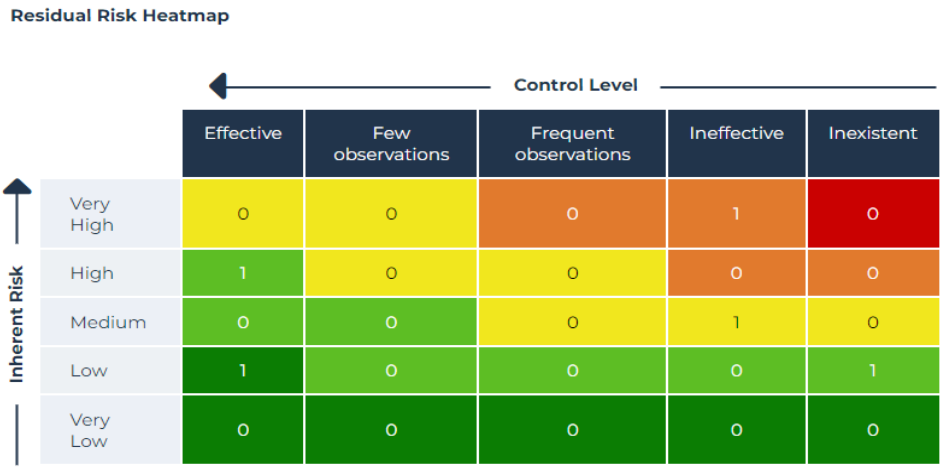
Controls by control level

A pie chart indicates the distribution of controls by control level:

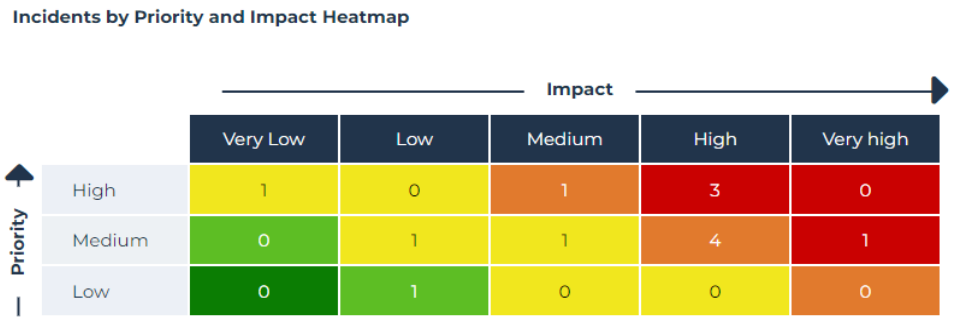
- Pass controls
- Fail controls
- Unassessed controls



Residual risk heatmap



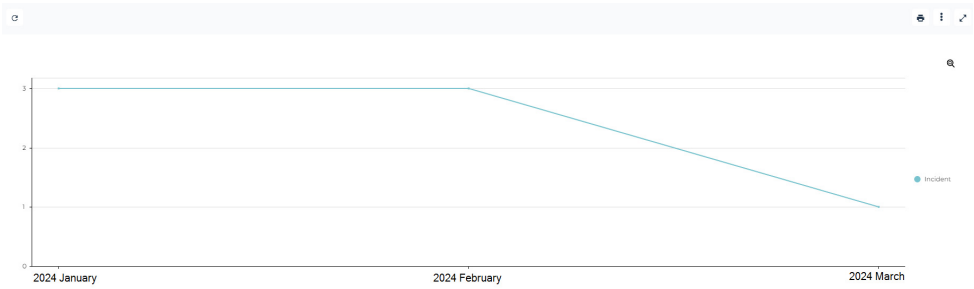
Incident heatmap by impact and priority



Evolutions of incidents over a year

A line chart represents the evolution of incidents over the year. It displays:

- horizontally, the month the incident was detected
- vertically, the number of incidents during this month



Process Criticality and Supporting ICT Assets Table Overview

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. Use filters to find the **Process Criticality and Supporting ICT Assets Table Overview** report.

Illustrations

Table / Matrix

Report parameters

Parameters	
List of processes	Optional
Entity	Mandatory

Report Content

This table presents:

- the result of the last BIA of the selected processes and entity
- the impact analysis displaying the list of ICT assets which support the processes

The following columns are available:

- **Processes**
- **Criticality level**: last criticality level computed on the BIA connected to the process and entity
- **ICT asset type**
  - Application
  - Software technology
  - Deployed server
  - Site
  - Data center
  - Facility
  - Vendor
- **ICT asset**: name of the ICT asset
- **Risk**: risk connected to the ICT asset at risk
- **Residual risk** : last residual risk on the risk with the ICT asset as a context
- **Risk action plan**: action plan connected to the control ("To be started" or "In progress" status)
- **Control**: control connected to the risk
- **Control level**
- **Control Action Plan**: action plan connected to the control ("To be started" or "In progress" status)

Example

Process	Criticality level	ICT Resource Type	ICT Resource	Risks	Residual Risk	Risk Action Plans	Controls	Control Level	Control Action Plans
* Screen and select candidates		Application	HR Management	Negative treasury					
				Unavailable Data Center due to Flood					
		Software Technology	Database - Standard Edition 2 (SE2) - 12.1.0.2						
			Office 2010						
			Office 2013						
			Oracle 11gR2						

VENDORS OVERVIEW BY PROCESS

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. Use filters to find the **Vendors Overview by Process** report.

Illustrations

Table / Matrix

Report parameters

Parameters	
Critical processes	Mandatory

A process is considered critical when at least one of the business impact values of the last BIA proved to be "Critical".

See Managing Business Impact Values for more information on the definition of the BIA template.

Report Content

This table presents a global overview of the vendors involved in the selected processes.

The following columns are available:

- **Critical process**
- **Entity**: entity of the BIA
- **BIA date**: BIA closure date
- **Business impact**
- **Contract**: ongoing contract
- **Contract type**
- **Code**
- **Vendor**: vendor involved in the process (with an ongoing contract)
- **Cyber rating**
- **Resource**
- **Contract begin date**
- **Contract end date**
- **Attachments** (number, with a link to the attachments)

Example

Critical Process	Entity	BIA Date	Business Impact	Contract	Contract Type	Code	Vendor	Cyber Rating	Asset	Contract Begin Date	Contract End Date	Attachments
* Find, select and recruit employees	France	9/19/2023	Medium	Contract-3			Adobe Systems		• * Find, select and recruit employees	10/1/2024	10/24/2024	0
Develop and manage the planning, regulations and HR strategy	France	9/19/2023	Medium									
Manage employee information	France	9/20/2023	Critical	Contract-1			Microsoft Azure		• * Apache log4j v2.17 • * MEGA BANK Mobile App • Manage employee information	10/15/2024	10/31/2024	0
Manage the Skills and Training of Employees	France	9/20/2023	Low									

CRITICAL ICT ASSETS (FROM PROCESS/ENTITY)

Path

To access this report:

1. In the navigation bar, click **Reports > Create a report**.
2. Use filters to find the **Critical ICT Assets (from Process/Entity)** report.

Illustration

Table / Matrix

Report parameters

Parameters	
Processes or Entity	Mandatory
Risk Type	Optional

Report Content

This report is displayed in the form of a table and contains the following columns:

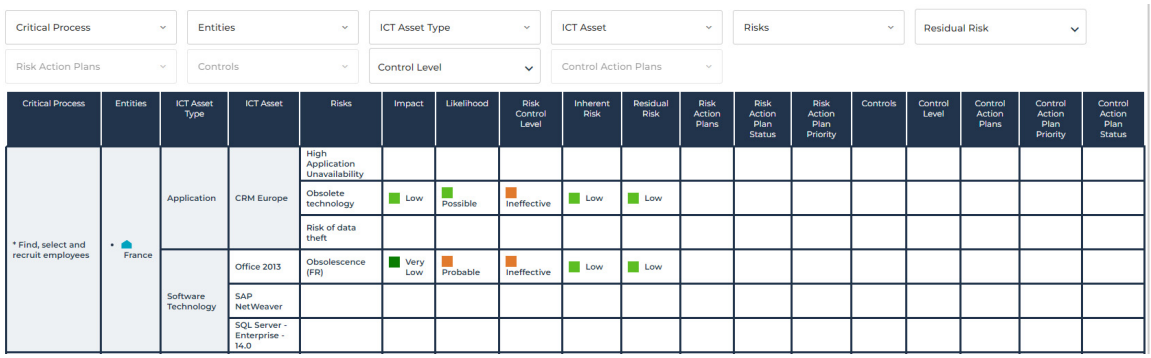
- **Critical process**

  A process is considered critical when at least one of the business impact values of the last BIA proved to be "Critical".

  See Managing Business Impact Values for more information on the definition of the BIA template.

- **Entities**
- **ICT asset type**
- **ICT asset**
- **Risk**
- **Impact**
- **Likelihood**
- **Inherent risk**
- **Control Level**
- **Residual risk**
- **Risk action plan**
- **Control**
- **Control level**
- **Control action plan**

Report example



Critical Process | Entities | ICT Asset Type | ICT Asset | Risks | Residual Risk
Risk Action Plans | Controls | Control Level | Control Action Plans

Critical Process	Entities	ICT Asset Type	ICT Asset	Risks	Impact	Likelihood	Risk Control Level	Inherent Risk	Residual Risk	Risk Action Plans	Risk Action Plan Status	Risk Action Plan Priority	Controls	Control Level	Control Action Plans	Control Action Plan Priority	Control Action Plan Status
* Find, select and recruit employees	• France	Application	CRM Europe	High Application Unavailability													
				Obsolete technology	Low	Possible	Ineffective	Low	Low								
				Risk of data theft													
		Software Technology	Office 2013	Obsolescence (FR)	Very Low	Probable	Ineffective	Low	Low								
			SAP NetWeaver														
			SQL Server - Enterprise - 14.0														