Hopex GRC

Hopex Aquila

Bizzdesign

Fonctionnalités communes GRC

Guide d’utilisation

Hopex Aquila

Bizzdesign

SOMMAIRE

BUREAU MANAGER GRC

Le bureau Hopex GRC (Governance, Risk & Compliance) constitue un point d'accès central pour les responsables des risques, contrôles, incidents et d'audit.

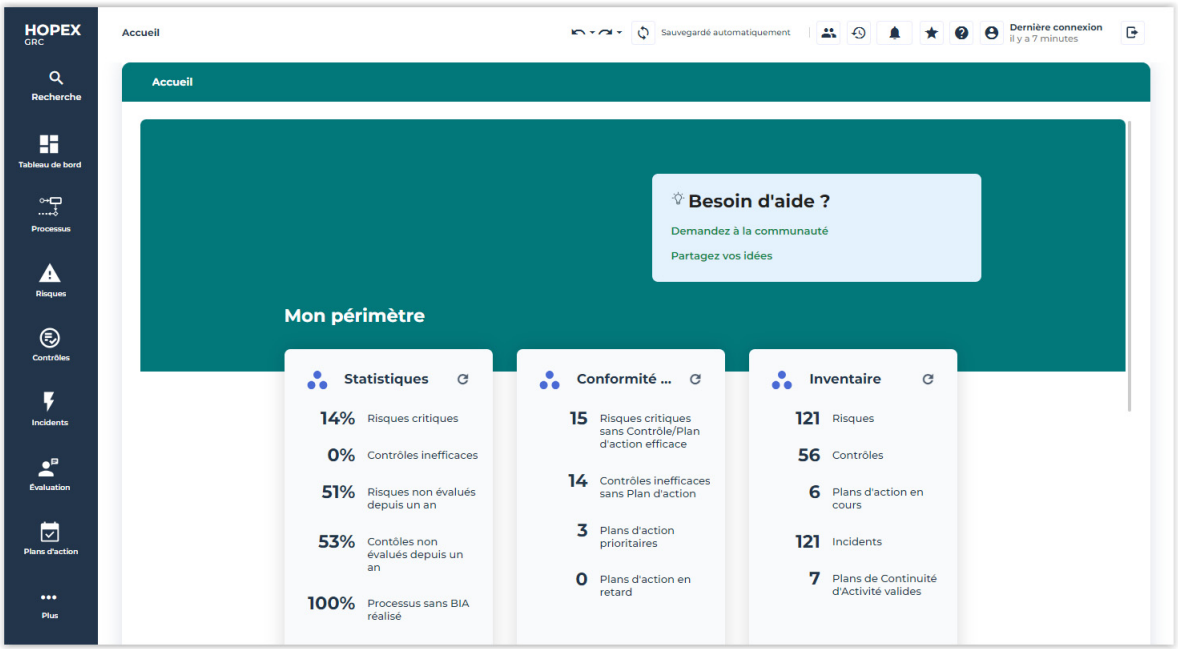
Il est disponible avec les produits suivants :

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

  ☛ *Plus de détails sur **Hopex Internal Audit**, voir la documentation correspondante.*
- **Hopex BCM**

Les fonctionnalités disponibles dépendent de la (des) solution(s) que vous utilisez ainsi que du profil avec lequel vous vous connectez.

Des menus concernent les principaux types d'objets de la GRC, ainsi que des types d'objets et fonctionnalités de la plateforme **Hopex.**



Recherche

Voir Recherche dans la section "Fonctionnalités communes".

Tableau de bord

Permet d’ajouter des widgets spécifiques à la gestion des risques et contrôles ainsi qu’à l’audit interne.

Processus

Voir Gérer les catégories de processus et processus.

Risques

Voir Gérer les risques.

Contrôles

Voir Gérer les contrôles.

Incidents

Voir Collecte des incidents.

Évaluation

Voir Campagnes d’évaluation.

Voir aussi la documentation spécifique à chaque solution :

- Évaluer les risques
- Exécuter les contrôles.
- Evaluer les contrôles

Plans d'action

Voir aussi : Gérer les défaillances et plans d'action.

Conformité

Voir Gérer la conformité.

Testing

Voir Tester les contrôles.

☛ *Ce menu concerne **Hopex Internal Control** seulement.*

Continuité

Ce menu concerne la continuité de l'activité.

Voir Introduction à Hopex BCM.

☛ *Ce menu concerne **Hopex BCM** seulement.*

Rapports

Voir Rapports des solutions GRC.

Environnement

Voir Environnement GRC.

☛ *Ce menu est disponible pour l'Administrateur fonctionnel GRC seulement.*

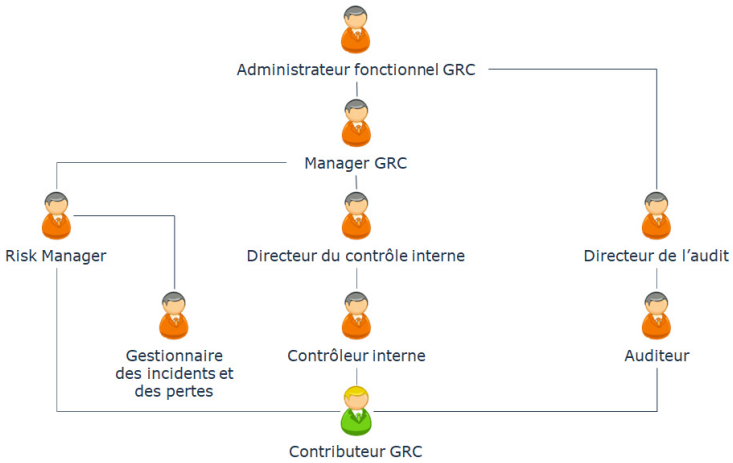
ACCÉDER AU BUREAU GRC

Pour se connecter à **Hopex**, voir Se connecter à Hopex.

Dans **Hopex GRC**, il existe, par défaut, des profils auxquels sont associées des activités spécifiques.

Les menus et commandes disponibles dans la solution dépendent du profil avec lequel vous êtes connecté.

Profils utilisés dans les solutions GRC



Risk Manager

Le Risk Manager est responsable de l'exécution des tâches suivantes concernant les risques de son domaine de responsabilité :

- identifier les risques
- réaliser des évaluations directes
- gérer les campagnes d'évaluation
- définir des plans d'action
- analyser et suivre la création de rapports

Pour plus de détails, voir Gérer les risques.

Directeur du contrôle interne

Le directeur du contrôle interne :

- possède les mêmes droits que les contrôleurs internes
  - ☛ *Voir Contrôleur interne.*
- valide les campagnes
- prépare les plans de test
- valide les plans d'action

Pour plus de détails, voir Gérer les contrôles (Hopex Internal Control)

Gestionnaire des incidents et des pertes

Le gestionnaire des incidents et des pertes crée les éléments nécessaires à la gestion des incidents et des pertes.

Il gère la description de l'environnement : acteurs et processus organisationnels, environnement réglementaire, ressources IT.

Il peut intervenir sur :

- les incidents déclarés
- les plans d'action et les actions

Pour plus de détails, voir Collecte des incidents (Hopex LDC).

Manager GRC

Le profil Manager GRC est disponible si vous possédez plusieurs solutions parmi :

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

Il regroupe les profils suivants (à condition de disposer des solutions correspondantes) :

- Risk Manager
- Directeur du contrôle interne
- Gestionnaire des incidents et des pertes

Contrôleur interne

Le contrôleur interne :

- définit les contrôles
- prépare les campagnes d'évaluation
- exécute les missions de test (créer les programmes de travail, les défaillances et les plans d'action)
- valide et suit les plans d'action

Administrateur fonctionnel GRC

L'administrateur fonctionnel GRC a accès aux mêmes menus que le Manager GRC, avec en complément des fonctionnalités globales d'administration (comme la gestion des utilisateurs).

> ☛ *L'administrateur fonctionnel GRC possède également les droits du Directeur d'audit.*

L'administrateur fonctionnel GRC :

- possède des droits sur tous les objets et workflows.
- prépare l'environnement de travail et crée les éléments nécessaires à la gestion des risques et contrôles.
- gère :
  - la description de l'environnement, notamment les acteurs et processus
  - l'environnement réglementaire
  - les ressources informatiques
  - les utilisateurs et l'assignation des profils

Contributeur GRC

Le contributeur effectue ses tâches dans un bureau simplifié. Pour plus de détails, voir Fonctionnalités disponibles pour le contributeur GRC.

Synthèse Profils / Solutions GRC

Solutions/ Profils	***ERM***	***IC***	***LDC***	***BCM***
Administrateur fonctionnel GRC	X	X	X	X
Manager GRC	X	X	X	X
Contributeur GRC	X	X	X	X
Risk Manager	X			X
Directeur du contrôle interne		X		
Contrôleur interne		X		
Gestionnaire des incidents et des pertes			X	

PRÉSENTATION DE LA DOCUMENTATION GRC

La documentation relative à GRC (Governance, Risk & Compliance) est articulée comme suit :

Fonctionnalités communes aux solutions GRC

- Environnement GRC
- Indicateurs clés
- Campagnes d'évaluation
- Rapports des solutions GRC

  ☛ *Pour les rapports concernant les risques/contrôles/incidents, voir :*

  - *Rapports concernant les risques*.
  - *Rapports concernant les contrôles*
  - *Rapports concernant les incidents*
- Workflows des solutions GRC
- Annexe - Règles de calcul

Hopex Internal Control

- Gérer les contrôles
- Evaluer les contrôles
- Exécuter les contrôles
- Gérer la conformité
- Tester les contrôles
- Rapports concernant les contrôles
- Gérer les défaillances et plans d'action
- Rapports concernant les contrôles

Hopex Enterprise Risk Management

- Gérer les risques
- Évaluer les risques
- Rapports concernant les risques

Hopex LDC

- Collecte des incidents
- Rapports concernant les incidents

Hopex BCM

- Gérer les systèmes de MCA
- Définir un Bilan d'Impact sur l'Activité
- Concevoir un Plan de Continuité d'Activité
- Tester un Plan de Continuité d'Activité
- Gérer les crises

ADMINISTRATION FONCTIONNELLE GRC

Afin que les différents participants puissent assumer leur rôle dans le cadre d'un projet GRC (Governance, Risk & Compliance), il est nécessaire de créer et gérer au préalable les éléments nécessaires à la préparation des tâches de chacun.

☛ *Vous devez vous connecter avec le profil "Administrateur fonctionnel GRC" pour réaliser ces tâches.*

- ✓ Réutiliser les données réglementaires
- ✓ Gérer les équipes
- ✓ Gérer les devises
- ✓ Paramétrer les feuilles de temps
- ✓ Gérer les calendriers de campagnes
- ✓ Gérer les calendriers de pilotage
- ✓ Administrer les indicateurs clés

RÉUTILISER LES DONNÉES RÉGLEMENTAIRES

Si votre référentiel contient des cadres réglementaires et exigences utilisés dans d'autres solutions, vous devez les convertir pour pouvoir les réutiliser dans **Hopex GRC**.

> 🕮 *Un cadre réglementaire représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.*
>
> 🕮 *Une exigence est un besoin ou une attente formulés explicitement, imposés comme une contrainte à respecter dans le cadre d'un projet de certification, d'organisation ou de modification du système d'information d'une entreprise.*

Type d'objet source	Type d'objet obtenu après conversion
Cadre réglementaire	Texte de référence
Exigence	Article + Obligation

> ☛ *Pour plus de détails sur les textes de référence, articles et obligations, voir Gérer le registre de conformité.*

Convertir les données réglementaires

Pour convertir les cadres réglementaires et exigences :

1. Dans la barre de navigation, cliquez sur **Administration > Outils > Conversion des données réglementaires**.
   Des jauges vous indiquent le pourcentage de cadres réglementaires et d'exigences qui ont été convertis jusqu'à présent.
2. Cliquez sur **Lancer la conversion des données**.
3. Dans la colonne **Convertir en**, indiquez, pour chaque cadre réglementaire, si vous voulez :
   - le convertir en texte de référence

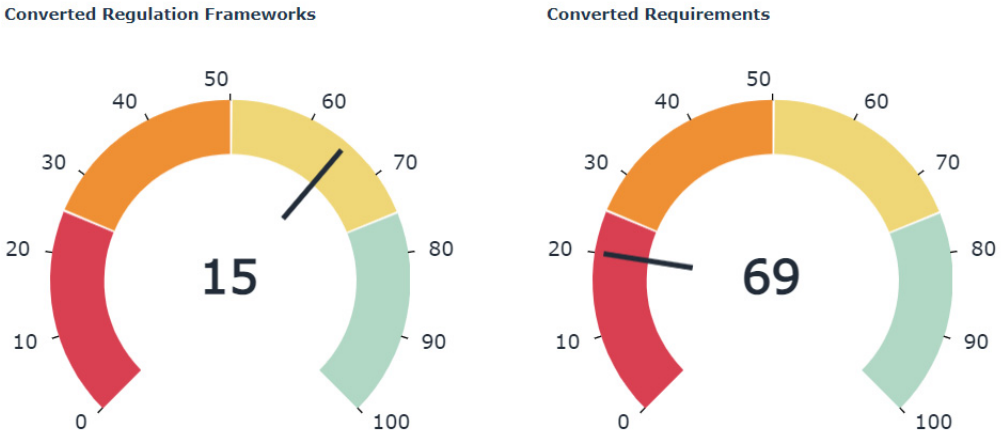
     > 🕮 *Un texte de référence est un texte qui entre dans l'une des catégories suivantes : réglementations (textes de lois qui peuvent entraîner des pénalités s'ils ne sont pas respectés), standards ou normes.*
   - le convertir en cadre de politiques d'entreprise

     > 🕮 *Un cadre de politique d'entreprise constitue un ensemble de politiques d'entreprise. Les cadres de politique d'entreprise peuvent contenir des sections.*
   - ne pas le convertir

     > ☛ *Par défaut, les Cadres réglementaires sont convertis en Textes de référence. Le bouton **Appliquer les paramètres de conversion par***

défaut *permet de revenir au paramétrage initial si vous avez effectué des changements.*

A la fin de la conversion, les jauges présentent le pourcentage actualisé.



Les données converties sont visibles dans le registre de conformité (menu **Conformité**). Pour plus de détails, voir Gérer le registre de conformité.

☛ *La date de la réglementation n'est pas convertie. De plus les caractéristiques personnalisées ne sont pas non plus converties.*

GÉRER LES ÉQUIPES

La gestion des équipes concernent les solutions suivantes :

- **Hopex Internal Control** (missions de test)
- **Hopex Internal Audit** (missions d'audit)

Avant de planifier les missions d'audit ou de test, il est nécessaire de constituer les équipes appropriées et d'attribuer les rôles et les responsabilités de chacun.

Vous devez au préalable avoir défini :

- des types de compétence
- une liste de compétences
- des niveaux de compétence.

Des outils permettent de créer et de visualiser les compétences des membres de l'équipe.

Créer des types de compétence

Pour créer un type de compétence :

1. Dans la barre de navigation, sélectionnez **Administration > Gestion des compétences > Types de compétence**.
2. Cliquez sur **Nouveau**.
3. Saisissez un **Nom** pour le type de compétence, par exemple "Langues".
4. Cliquez sur **OK**.

Créer des compétences

Pour créer une compétence :

1. Dans la barre de navigation, sélectionnez **Administration > Gestion des compétences > Compétences**.
2. Cliquez sur **Nouveau**.
3. Saisissez le **Nom** de la compétence, par exemple "Anglais".
4. Cliquez sur **OK**.
   La liste des compétences est enrichie de la nouvelle compétence.
   Dans les propriétés de la compétence, vous pouvez indiquer le **Type de compétence** auquel elle se rattache, par exemple "Langues".

Créer des niveaux de compétence

Vous devez maintenant créer des niveaux de compétence sur chaque type de compétence.

Pour créer un niveau de compétence :

1. Dans la barre de navigation, sélectionnez **Administration > Gestion des compétences > Types de compétence**.
2. Ouvrez les propriétés du type de compétence qui vous intéresse.
3. Dans la section **Niveaux de compétence**, cliquez sur **Nouveau**.
4. Saisissez un **Nom**, par exemple "Débutant"".

5. Cliquez sur **OK**.
6. Dans le champ **Code du niveau de compétence**, saisissez un chiffre correspondant au niveau de compétence, par exemple "1" pour "Débutant" (alors que "4" pourrait correspondre à "Confirmé" dans notre exemple).

   ☛ *Ce chiffre permet de visualiser graphiquement l'étendue des compétences du contrôleur dans la page d'affectation des missions de test.*

Visualiser les compétences de chaque utilisateur

Pour visualiser les compétences d'un utilisateur :

1. Dans la barre de navigation, sélectionnez **Administration > Gestion des compétences > Compétences utilisateur**.
2. Sélectionnez un utilisateur et cliquez sur le bouton **Compétences des personnes**.
   La page de compétences de l'utilisateur sélectionné s'ouvre.

GÉRER LES DEVISES

Les devises sont utilisées :

- lors de la saisie des pertes d'incidents
- dans le cadre des missions de test ou d'audit pour la saisie des notes de frais.

Il convient de distinguer deux types de devise :

- la devise centrale

  La devise centrale est la devise retenue par l'entreprise comme devise de référence.

- la devise locale

  Une devise locale est définie pour chaque utilisateur. Il s'agit par défaut de la devise centrale.

Définir la devise centrale

Pour définir la devise centrale :

1. Dans l'application d'administration (administration.exe), connectez-vous à l'environnement dans lequel vous souhaitez travailler.
2. Faites un clic droit sur le référentiel et sélectionnez **Options > Modifier**. La fenêtre des options du référentiel s'ouvre.
3. Cliquez sur le dossier **Installation > Devise**. La fenêtre de droite présente la liste des devises disponibles en standard.
4. Dans le champ **Symbole monétaire** spécifiez le symbole de votre devise de consolidation, par exemple "$".
5. Dans le champ **Devise centrale** sélectionnez votre devise de consolidation, par exemple "US Dollar".
6. Cliquez sur **Ok**.
7. Quittez l'application d'administration.

Définir les devises locales proposées aux utilisateurs

L'administrateur fonctionnel GRC doit définir les devises locales qui seront proposées aux utilisateurs.

(**Hopex Windows Front-End**) Pour définir la liste des devises locales :

1. Dans le dossier où **Hopex** est installé, lancez "Administration.exe" et connectez-vous avec un utilisateur qui dispose de l'autorisation d'administration des données.
2. Sélectionnez l'environnement puis le référentiel sur lequel vous souhaitez travailler.
3. Faites un clic droit sur le référentiel et sélectionnez **Options**. La fenêtre des options du référentiel s'ouvre.
4. Cliquez sur le dossier **Installation > Devise**. La fenêtre de droite présente la liste des devises disponibles en standard.
5. Cochez ensuite toutes les devises qui seront utilisées en local par vos utilisateurs.

6. Cliquez sur **Ok**.
7. Quittez l'application d'administration.

(**Hopex Web Front-End**) Pour définir la liste des devises locales :

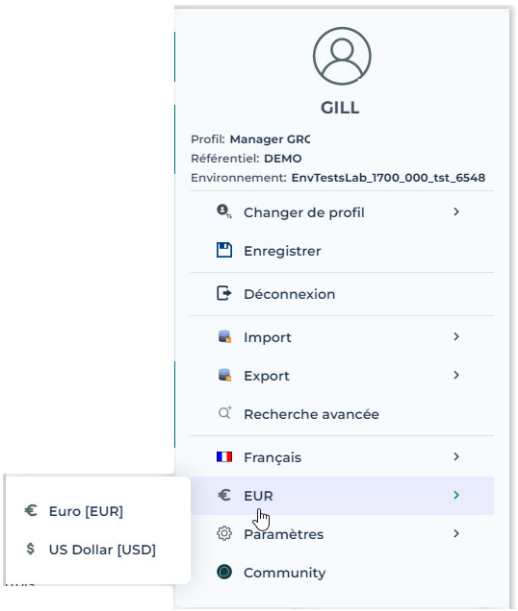
1. Connectez-vous avec le profil "Administrateur fonctionnel GRC".
2. Dans le menu principal, sélectionnez **Paramètres > Options**.
3. Cliquez sur le dossier **Installation > Devise**.
   La fenêtre de droite présente la liste des devises disponibles en standard.
4. Cochez toutes les devises qui seront utilisées en local par vos utilisateurs.
5. Cliquez sur **Ok**.

Spécifier votre devise locale

En tant qu'utilisateur, vous pouvez choisir une devise locale différente de la devise centrale.

Pour modifier votre devise locale :

- Dans le menu principal, sélectionnez une devise, comme ci-dessous.



Gérer les taux de change

Pour saisir un taux de change :

1. Dans la barre de navigation, sélectionnez **Administration > Outils > Taux de change**.
2. Cliquez sur **Nouveau**.

3. Dans la fenêtre qui apparaît, saisissez :
   - le **Code de la devise finale**
   - le **Taux** de change de la devise d'origine par rapport à la devise finale.
   - la **Date de début du taux**.

     ☛ *Plusieurs périodes de taux de change peuvent être saisies pour une même devise. Lors de la saisie des dépenses, le taux de change le plus récent est pris en compte.*

     ☛ *Vous devez saisir le taux de change dans les deux sens, par exemple :*

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

Pour visualiser un taux de change :

1. Dans les listes déroulantes situées au-dessus du tableau, sélectionnez la devise source et la devise finale.
2. Cliquez sur le bouton **Rafraîchir**.
   Les taux de change pour la devise sélectionnée apparaissent.

   ☛ *Pour inverser le taux de change, cliquez sur le bouton* 

PARAMÉTRER LES FEUILLES DE TEMPS

Les feuilles de temps sont utilisées dans le cadre des missions d'audit/de test.

L'administrateur fonctionnel GRC peut paramétrer les options par défaut de gestion des feuilles de temps.

L'administrateur fonctionnel GRC peut définir :

- le nombre d'heures travaillées par jour
- les jours non travaillés dans l'entreprise

Pour paramétrer ces données :

1. A partir du menu principal, sélectionnez **Paramètres > Options**.
2. Dans la fenêtre qui apparaît, dépliez les dossiers **Installation > Gestion des utilisateurs**.
3. Dans la partie droite de la fenêtre précisez :
   - le nombre d'**Heures/jour** pour chaque auditeur.
     ☛ *La valeur par défaut est "8".*
   - les jours correspondant au week-end
     ☛ *Les valeurs par défaut sont "samedi" et "dimanche".*

Gérer les calendriers de campagnes

Un calendrier est divisé en périodes de temps appelées périodes de calendrier. Les calendriers peuvent servir dans le cas des campagnes d'évaluation, de la génération de rapports, ainsi que pour planifier les missions d'audit/de test.

☛ *Un calendrier couvre souvent une période d'un an, qu'il s'agisse d'un exercice fiscal ou d'une année calendaire. Dans ce dernier cas, une période de calendrier peut correspondre à un trimestre.*

Créer un calendrier

Pour créer un calendrier :

1. Dans la barre de navigation, cliquez sur **Administration > Calendriers > Calendriers**.
2. Cliquez sur **Nouveau**.
3. Saisissez le **Nom** du calendrier, ainsi que les dates de début et de fin.
4. Cliquez sur **OK**.

Vous pouvez ensuite définir les périodes de calendrier.

Créer les périodes de calendrier

Pour créer les périodes de calendrier :

1. Ouvrez les **Propriétés** du calendrier.
2. Dans la section **Périodes de calendrier,** cliquez sur **Nouveau**.
3. Saisissez le **Nom** de la période de calendrier, ainsi que ses dates de début et de fin.
4. Cliquez sur **OK**.
5. Créez de la même manière d'autres périodes de calendrier.

Le calendrier est créé. Il peut ensuite être relié à un plan d'audit ou de test.

Relier un calendrier à un plan d'audit ou de test

Pour relier un calendrier à un plan d'audit ou de test :

1. Dans la barre de navigation, cliquez sur :
   - **Audits > Plans d'audit**.
   - **Testing > Plans de test**.
2. Ouvrez les propriétés du plan qui vous intéresse.
3. Cliquez sur **Caractéristiques**.
4. Dans le champ **Calendrier**, sélectionnez le calendrier à relier.

GÉRER LES CALENDRIERS DE PILOTAGE

Les calendriers de pilotage sont utilisés dans le cadre :

- des campagnes d'exécution

  ☛ *Voir Préparer l'exécution des contrôles.*

- des rappels sur les plans d'action

Pour créer et paramétrer un calendrier de pilotage :

1. Dans la barre de navigation, sélectionnez **Administration > Calendriers > Calendriers de pilotage**.
2. Cliquez sur **Nouveau**.
3. Dans l'assistant qui apparaît, sélectionnez le cadre dans lequel vous voulez utiliser le calendrier de pilotage :
   - Contrôle
   - Indicateur clé
   - Plan d'action
   - Recommandation
4. Reliez une **Date de pilotage** (correspondant à la fréquence d'exécution qui vous intéresse).
5. Ouvrez la fenêtre de propriétés de la date de pilotage et cliquez sur l'onglet **Planification**.
6. Renseignez les informations nécessaires au lancement de la campagne dont :
   - le fuseau horaire à prendre en compte (UTC, fuseau horaire de l'utilisateur, fuseau horaire du serveur)
   - les dates de début de la récurrence.

     ☛ *La date de début spécifiée sur le calendrier de pilotage ne représente pas la date de démarrage de la campagne. Elle permet seulement de définir l'intervalle dans lequel la session d'évaluation peut avoir lieu.*

     ☛ *Il est conseillé d'utiliser une date de début relative sur la date de pilotage.*

   - la date et l'heure de démarrage.

     ☛ *Pour des détails sur les paramétrages possibles, voir la partie concernant le planificateur (scheduler) dans l'article technique "HOPEX Studio".*

     ☛ *Cochez la case **Exécuter à la date / heure de démarrage** si vous souhaitez lancer immédiatement une campagne d'exécution.*

     Si la case est désactivée, le planificateur attend la prochaine date (et heure) récurrente pour lancer le job.

ADMINISTRER LES INDICATEURS CLÉS

En tant qu'administrateur fonctionnel GRC, vous pouvez être amené à personnaliser la façon de définir les indicateurs clés (via des macros pour calculer le temps avant défaillance et les statuts, ou pour définir les périodes et méthodes d'agrégation).

Les indicateurs clés sont utilisés dans **Hopex Enterprise Risk Management** et **Hopex Internal Control**.

Accéder à l'administration des indicateurs clés

Pour accéder aux fonctionnalités d'administration des indicteurs clés :

1. Connectez-vous avec le profil "Administrateur fonctionnel GRC".
2. Dans la barre de navigation, sélectionnez **Administration > Indicateurs**.

Vous pouvez visualiser :

- les catégories d'indicateurs

  La catégorie d'indicateur clé détermine la façon dont les valeurs de l'indicateur sont interprétées, de façon à obtenir le statut de l'indicateur et le temps avant défaillance.

- les logiques d'interprétation

  Une logique d'interprétation d'indicateur contient la logique de calcul du statut de l'indicateur, le temps avant défaillance, ainsi que la liste des statuts dans lesquels l'indicateur peut se trouver.

- les statuts d'indicateurs

  Le statut d'un indicateur permet de déterminer si une alerte doit être déclenchée. L'indicateur est calculé automatiquement en se basant sur les dernières valeurs de l'indicateur, la période d'agrégation et la méthode d'agrégation.

- les périodes d'agrégation

  La période d'agrégation est la période au cours de laquelle les valeurs de l'indicateur clé sont agrégées, de manière à calculer sa valeur et son statut.

- les méthodes d'agrégation

  Une méthode d'agrégation est une opération mathématique réalisée sur les valeurs agrégées de l'indicateur clé, de manière à calculer la valeur de ce dernier ainsi que son statut.

Définir des catégories d'indicateurs clés

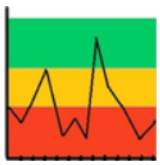
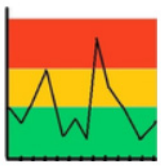
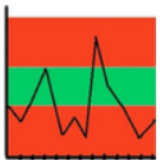
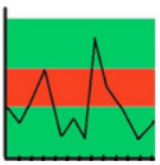
La catégorie d'indicateur clé détermine la façon dont les valeurs de l'indicateur sont interprétées, de façon à obtenir le statut de l'indicateur et le temps avant défaillance.

Pour visualiser les catégories d'indicateurs clés :

- Dans la barre de navigation, sélectionnez **Administration > Indicateurs > Catégories**.

Dans la page de propriétés des indicateurs clés, vous pouvez modifier la macro utilisée pour définir le temps avant défaillance.

> 🕮 *Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".*
>
> ☛ *La macro utilisée pour définir les statuts est définie sur les logiques d'interprétation d'indicateurs clés. Pour plus de détails, voir Définir les logiques d'interprétation d'indicateurs clés.*

Catégorie d'indicateur clé	Explication	Explication visuelle
Standard	La limite haute est utilisée pour définir l'objectif de l'indicateur clé, c'est-à-dire les valeurs acceptées. Toutes les valeurs supérieures à l'objectif sont acceptées.	
Inversé	La limite basse est utilisée pour définir l'objectif de l'indicateur clé, c'est-à-dire les valeurs acceptées. Toutes les valeurs inférieures à l'objectif sont acceptées.	
Valeurs acceptées	Les limites haute et basse sont utilisées pour définir la plage de valeurs acceptées. Toutes les valeurs en-dehors de cette plage sont exclues.	
Valeurs exclues	Les limites haute et basse sont utilisées pour définir la plage de valeurs exclues. Toutes les valeurs en-dehors de cette plage sont acceptées.	

Définir les logiques d'interprétation d'indicateurs clés

> 🕮 *Une logique d'interprétation d'indicateur contient la logique de calcul du statut de l'indicateur, le temps avant défaillance, ainsi que la liste des statuts dans lesquels l'indicateur peut se trouver.*

Vous pouvez créer plusieurs logiques d'interprétation d'indicateur clé pour chaque catégorie d'indicateur. Il peut en effet être utile de proposer différentes règles de calcul pour chaque catégorie d'indicateur clé.

Pour créer des logiques d'indicateur clé :

1. Dans la barre de navigation, sélectionnez **Administration > Indicateurs > Logiques d'interprétation**.
2. Cliquez sur **Nouveau**.
3. Dans la fenêtre qui s'affiche, spécifiez la **Catégorie d'indicateur** à laquelle vous voulez rattacher la logique.
4. Spécifiez la **Macro** utilisée pour calculer les statuts d'indicateur clé.

   ☛ *La macro utilisée pour calculer le temps avant défaillance est définie sur la catégorie d'i'ndicateur clé. Pour plus de détails, voir Définir des catégories d'indicateurs clés.*
5. Dans le champ **Statuts d'indicateurs**, sélectionnez les différents statuts disponibles pour les indicateurs clés qui utilisent cette logique d'interprétation.
6. Cliquez sur **OK**.

Définir des statuts d'indicateurs clés

Le statut d'un indicateur permet de déterminer si une alerte doit être déclenchée. L'indicateur est calculé automatiquement en se basant sur les dernières valeurs de l'indicateur, la période d'agrégation et la méthode d'agrégation.

Créer des statuts d'indicateurs clés

Pour créer des statuts d'indicateurs clés :

1. Dans la barre de navigation, sélectionnez **Administration > Indicateurs > Statuts**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez une **Couleur de statut** pour votre nouveau statut.
4. Cliquez sur **OK**.

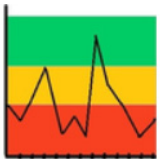
Le statut que vous venez de créer apparaît dans la liste des statuts disponibles au moment de créer une logique d'interprétation d'indicateur clé. Pour plus de détails, voir Définir les logiques d'interprétation d'indicateurs clés.

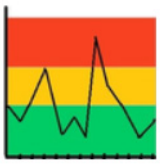
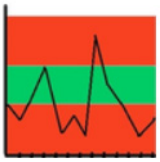
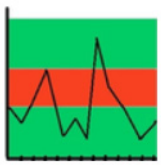
Calcul des statuts d'indicateurs

Les statuts suivants sont disponibles par défaut :

- Non connu
- Satisfaisant
- Acceptable (avec avertissement)
- Insatisfaisant
- Critique
- Non acceptable

Le statut de l'indicateur est calculé via une logique d'interprétation d'indicateur reliée à une catégorie d'indicateur. Ci-après figurent les règles de calcul applicables à la logique d'interprétation standard.

Logiques d'interprétation	**Détails**	**Représentation visuelle**
Standard	Règle par défaut permettant de calculer le statut des indicateurs clés de catégorie Standard. Le statut de l'indicateur clé est Non acceptable pour toute valeur inférieure à la limite basse. Pour les valeurs supérieures à cette limite, le statut va de Critique à Satisfaisant, en passant par Insatisfaisant et Acceptable (avec avertissement). Le statut de l'indicateur clé est Satisfaisant pour les valeurs supérieures à la limite basse + 0,75*(limite haute - limite basse).	

Logiques d'interprétation	Détails	Représentation visuelle
Inversé	Règle par défaut permettant de calculer le statut des indicateurs clés de catégorie Inversé. Cette règle met en oeuvre la logique inverse à celle utilisée pour les indicateurs clés de catégorie Standard. Le statut d'un indicateur clé est "Non acceptable" pour toute valeur dépassant la limite haute. Pour les valeurs inférieures à la limite haute, la statut va de Critique à Satisfaisant, en passant par Insatisfaisant et Acceptable (avec avertissement). Le statut de l'indicateur clé est Satisfaisant pour les valeurs inférieures à la limite haute - 0,75*(limite haute - limite basse).	
Valeurs acceptées	Règle par défaut permettant de calculer le statut des indicateurs clés de catégorie Valeurs acceptées. Le statut de l'indicateur clé est Non acceptable pour toute valeur qui trouve au-delà des limites définies. Concernant les valeurs à l'intérieur des limites, et, au fur et à mesure que la valeur de l'indicateur clé s'éloigne du centre, le statut va de Satisfaisant à Critique, en passant par Acceptable (avec avertissement) et Insatisfaisant. Le statut de l'indicateur clé est Satisfaisant pour les valeurs qui se situent dans l'intervalle (limite haute + limite basse)/2 +/- 0,25*(limite haute - limite basse).	
Valeurs exclues	Règle par défaut permettant de calculer le statut des indicateurs clés de catégorie Valeurs exclues. Le statut d'un indicateur clé est Non acceptable pour toute valeur qui se trouve dans les limites définies. Concernant les valeurs au-delà des limites, et au fur et à mesure que la valeur s'éloigne de ces limites, le statut de l'indicateur clé va de Critique à Satisfaisant, en passant par Insatisfaisant et Acceptable (avec avertissement). Le statut de l'indicateur clé est Satisfaisant pour les valeurs supérieures à la limite haute + 0,25*(limite haute - limite basse) (ou inférieures à la limite basse - 0,25*(limite haute - limite basse)).	

Formules des statuts d'indicateurs

```
M = (Limite basse + Limite haute)/2
Bas = limite basse
Haut = limite haute
```

Catégorie standard

Le statut de l'indicateur clé s'améliore au fur et à mesure que les valeurs augmentent.

Statut	Formule
Non connu	Valeurs non disponibles
Non acceptable	KI < Bas
Satisfaisant	KI >= Bas + 1,5*(Haut-M)
Acceptable (avec avertissement)	KI < Bas + 1,5*(Haut-M) ET KI >= Bas + 0,75*(Haut-M)
Insatisfaisant	KI < Bas + 0,75*(Haut-M) ET KI >= Bas + 0,25*(Haut-M)
Critique	KI < Bas + 0,25*(Haut-M) ET KI >= Bas

Catégorie Valeurs acceptées

Statut	Formule
Non connu	Valeurs non disponibles
Non acceptable	KI > Haut OU KI < Bas
Satisfaisant	KI >= M - 0,5*(Haut-M) ET KI <= M + 0,5*(Haut-M)
Acceptable (avec avertissement)	KI > M + 0,5*(Haut-M) ET KI <= M + 0,75*(Haut-M) OU KI < M - 0.5*(Haut-M) ET KI >= M - 0,75*(Haut-M)
Insatisfaisant	KI > M + 0,75*(Haut-M) ET KI < M + 0,9*(Haut-M) OR KI < M - 0,75*(Haut-M) ET KI > M - 0,9*(Haut-M)
Critique	KI > M + 0,9*(Haut-M) ET KI <= Haut OU KI < M - 0,9*(Haut-M) ET KI >= Bas

Catégorie Valeurs exclues

Statut	Formule
Non connu	Valeurs non disponibles
Non acceptable	KI <= Haut ET KI >= Bas
Satisfaisant	KI < Bas - 0,5*(Haut-M) OU KI >= Haut + 0,5*(Haut-M)

Statut	Formule
Acceptable (avec avertissement)	KI < Haut + 0,5*(Haut-M) ET KI >= Haut + 0,25*(Haut-M) OR KI >= Bas - 0,5*(Haut-M) ET KI < Bas - 0,25*(Haut-M)
Insatisfaisant	KI < Haut + 0,25*(Haut-M) ET KI >= Haut + 0,1*(Haut-M) OU KI >= Bas - 0,25*(Haut-M) ET KI < Bas- 0,1*(Haut-M)
Critique	KI > Haut ET KI < Haut + 0,1*(Haut-M) OR KI < Bas ET KI >= Bas - 0,1*(Bas-M)

Catégorie Inversé

Le statut de l'indicateur clé s'améliore au fur et à mesure que les valeurs baissent.

Statut	Formule
Non connu	Valeurs non disponibles
Non acceptable	KI > Haut
Satisfaisant	KI <= Haut – 1.5*(Haut-M)
Acceptable (avec avertissement)	KI > Haut – 1,5*(Haut-M) ET KI <= Haut – 0,75*(Haut-M)
Insatisfaisant	KI > Haut – 0,75*(Haut-M) ET KI <= Haut – 0,25*(Haut-M)
Critique	KI > Haut – 0,25*(Haut-M) ET KI <= Haut

Définir les périodes et les méthodes d'agrégation

Périodes d'agrégation

La période d'agrégation est la période au cours de laquelle les valeurs de l'indicateur clé sont agrégées, de manière à calculer sa valeur et son statut.

Les périodes d'agrégation suivantes sont disponibles par défaut :

- Hebdomadaire
- Bi-mensuelle
- Mensuelle
- Trimestrielle
- Semestrielle
- Annuelle

Méthodes d'agrégation

Une méthode d'agrégation est une opération mathématique réalisée sur les valeurs agrégées de l'indicateur clé, de manière à calculer la valeur de ce dernier ainsi que son statut.

Les méthodes d'agrégation suivantes sont disponibles par défaut :

- somme
- moyenne
- max
- min

Créer des périodes ou méthodes d'agrégation

Pour créer des périodes ou méthodes d'agrégation :

1. Dans la barre de navigation, sélectionnez **Administration > Indicateurs > Périodes d'agrégation/Méthodes d'agrégation**.
2. Cliquez sur **Nouveau**.
3. Dans l'assistant de création, reliez une **Macro**.
4. Cliquez sur **OK**.

Définir les logiques de calcul des valeurs d'indicateurs clés

Vous pouvez définir des logiques de calcul de valeurs d'indicateurs clés.

Créer une logique de calcul

Pour créer votre propre logique de calcul :

1. Dans la barre de navigation, sélectionnez **Administration > Indicateurs > Logiques de calcul des valeurs**.
2. Cliquez sur **Nouveau**.
3. Dans la fenêtre de propriétés de la logique ainsi créée, spécifiez :
   - une **Macro**.
   - (optionnel) les **Paramètres de calcul**

Logiques de calcul fournies par défaut

Logique de calcul via une requête

Cette logique de calcul vise à compter le nombre d'objets retournés par une requête.

Elle accepte deux paramètres :

- "Query" (obligatoire)
- "ObjectParameter" (facultatif) : si une requête exige un objet en paramètre, vous pouvez le spécifier via ce paramètre.

Calcul de pourcentage via requête

Cette logique de calcul compte le nombre d'objets retournés par des requêtes et calcule un pourcentage :

"NumeratorQuery" / "DenominatorQuery" * 100%

Elle accèpte 3 paramètres :

- "NumeratorQuery" (obligatoire)
- "DenominatorQuery" (facultatif)
- "ObjectParameter" (facultatif)

Condition	Résultat ou action
Si "DenominatorQuery" non spécifié	Dénominateur = nombre total d'objets du même type que le numérateur.
Si "NumeratorQuery" exige un objet en paramètre	Spécifiez le paramètre via "ObjectParameter"
Si "DenominatorQuery" exige un objet en paramètre	Spécifiez le même paramètre que pour "NumeratorQuery"

"RoundPrecision" définit la précision de l'arrondi (nombre de chiffres après la virgule).

Si le dénominateur est 0, la valeur calculée sera 0.

ENVIRONNEMENT GRC

Cette section présente comment visualiser votre environnement dans le bureau **Hopex GRC** (Governance, Risk & Compliance).

☛ *Certains types d'objets de l'environnement ou les caractéristiques présentées peuvent ne pas être utilisés dans toutes les solutions.*

- ✓ L'organisation
- ✓ L'environnement financier
- ✓ L'environnement stratégique
- ✓ L'environnement des risques
- ✓ L'environnement des contrôles
- ✓ L'environnement de conformité
- ✓ Les responsabilités (RACI)

L'ORGANISATION

L'organisation de l'entreprise est articulée autour des concepts suivants :

- entités : voir Gérer les entités
- processus : Gérer les catégories de processus et processus
- lignes métier : Gérer les lignes métier
- applications : Gérer les applications
- sites : Gérer les sites

Gérer les entités

Pour définir la liste des entités de votre organisation, **Hopex** vous permet de saisir l'organigramme de l'entreprise.

📖 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.*

Accéder aux entités de l'organisation

Pour accéder aux différentes entités de l'organisation :

❱ Dans la barre de navigation, sélectionnez **Processus > Par entités**.
La liste des entités composant l'organisation s'affiche.

☛ *La liste des entités détenues par une entité est accessible dans la page de propriétés de l'entité, dans la section **Sous-Entités**.*

Créer une entité

Pour créer une entité :

1. Voir Accéder aux entités de l'organisation.
2. Cliquez sur **Nouveau**.

Créer une sous-entité

Pour créer une sous-entité :

1. Voir Créer une entité.
2. Déplacez-là sous l'entité mère via un glisser-déposer dans l'arborescence.

Définir les caractéristiques générales d'une entité

Dans la fenêtre de propriétés d'une entité, vous pouvez préciser :

- son **Niveau** au sein de l'organisation :
  - Division
  - Département
  - Service.
- son **Statut** :
  - Actif
  - Inactif
- son **Type** :
  - Fournisseur

    ☛ *Le Fournisseur est nécessairement une entité "Externe".*
  - Institution
  - Société
  - Département public
  - Structure
  - Fonction
  - Générique
  - Responsable
- si l'entité est "Interne" ou "Externe"

  ☛ *Un Fournisseur est un exemple d'entité Externe.*
- son **Code**

  ☛ *Le champ **Entité mère** est calculé automatiquement en fonction de la position de l'entité dans l'arbre.*

Spécifier les responsabilités au sein d'une entité

Vous pouvez spécifier les personnes responsables au sein de l'entité.

Vous pouvez spécifier différents rôles au sein d'une entité :

- **Risk Manager** : personne chargée de la gestion des risques qui ont un impact sur l'entité

  🕮 *Le Risk Manager est responsable de l'exécution des tâches suivantes concernant les risques de son domaine de responsabilité : identifier les risques, réaliser des évaluations directes, gérer les*

campagnes d'évaluation, définir des plans d'action, analyser et suivre la création de rapports.

- **Correspondant Risque** : personne chargée de répondre aux questionnaires d'évaluation concernant les risques reliés à cette entité.

  ☛ *Vous pouvez définir plusieurs correspondants Risque sur une même entité.*

  🕮 *Le correspondant Risque est responsable de l'évaluation des risques de son périmètre, ainsi que de la mise en œuvre des plans d'action relatifs à ces risques.*

- **Correspondant Contrôle** : personne chargée de répondre aux questionnaires d'évaluation concernant les contrôles reliés à cette entité.

  ☛ *Vous pouvez définir plusieurs correspondants Contrôle sur une même entité.*

  🕮 *Le correspondant Contrôle est responsable de l'évaluation et de l'exécution des contrôles de son périmètre ainsi que de mise en œuvre des plans d'action relatifs à ces contrôles.*

- **Approbateur d'incident** : personne chargée de l'approbation des incidents qui ont un impact sur l'entité.
- **Déclarant d'incident :** Le déclarant d'incident est responsable de la création d'incidents de son périmètre.

  ☛ *Pour plus de détails, voir Le processus de gestion d'un incident.*

  ☛ *Le déclarant d'incident spécifié ici n'aura pas besoin de spécifier une entité de rattachement lorsqu'il sera amené à déclarer un incident.*

- **Membre de l'organisation** : ce rôle permet d'affecter un utilisateur à une entité.

  Exemple de cas d'utilisation : faire apparaître un utilisateur dans l'organigramme, spécifier des contacts pour un fournisseur.

Pour spécifier une responsabilité, par exemple un Correspondant Risque :

1. Dans la fenêtre de propriétés de l'entité concernée, dépliez la section **Responsabilités**.
2. Dans l'onglet **Correspondant Risque**, cliquez sur **Nouveau** pour définir une nouvelle responsabilité.
3. Sélectionnez une personne et cliquez sur **OK**.

Définir le périmètre d'une entité

Une entité peut être reliée à différents type d'objets.

Une page correspondant aux types d'objet suivants est disponible dans la page de propriétés de l'entité :

- **Risques**, dont la gestion est confiée à l'entité.

  ☛ *Pour plus de détails, voir Gérer les risques.*

- **Contrôles**, dont la gestion est confiée à l'entité.

  ☛ *Pour plus de détails, voir Gérer les contrôles.*

- **Incidents**
- **Plans d'action**

Une section correspondant aux types d'objet suivants est disponible dans la page **Caractéristiques** des propriétés de l'entité :

- **Entités** : vous pouvez spécifier l'entité responsable d'un service ou d'une direction ainsi que la dépendance fonctionnelle entre deux entités.
- **Processus** pour lesquels l'entité intervient.

  ☛ *Pour plus de détails, voir Gérer les catégories de processus et processus.*
- **Objectifs** assignés à l'entité.

  ☛ *Pour plus de détails, voir L'environnement stratégique.*
- **Lignes métier** pour lesquelles l'entité intervient.

  ☛ *Pour plus de détails, voir Gérer les lignes métier.*

Gérer les catégories de processus et processus

Deux niveaux de processus sont disponibles :

- catégorie de processus

  🕮 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*
- processus

  🕮 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

Accéder aux processus

Pour accéder à l'arbre des catégories de processus / processus:

❱ Dans la barre de navigation, sélectionnez **Processus**.

Les processus et catégories de processus apparaissent.

Hiérarchie de processus

La hiérarchie des processus/opérations se présente comme suit :

Catégorie de processus > Processus > Opération

Pour chaque processus de la hiérarchie sont affichés :

- les risques (directement reliés aux processus)
  - les contrôles (reliés aux risques, eux-mêmes reliés aux processus)
- les contrôles (directement reliés aux processus)

Les colonnes suivantes sont disponibles :

- **Risques** (nombre de)
- **Contrôles** (nombre de)
- **Dernière évaluation**
- **Risque résiduel**

  Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.
- **Risque prévisionnel**

  Le risque prévisionnel représente la projection du risque résiduel sur l'année à venir.
- **Dernier taux de conformité**

  Le taux de conformité est le pourcentage de contrôles jugés satisfaisants.
- **Niveau de contrôle**

  Le niveau de contrôle permet de caractériser le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour atténuer le risque.

Spécifier les caractéristiques d'un processus

Pour accéder aux caractéristiques d'un processus ou d'une catégorie de processus :

- Ouvrez la page **Caractéristiques** de sa fenêtre de propriétés.

Le **Propriétaire** est la personne qui a créé le processus. Elle est responsable du pilotage et du fonctionnement global du processus en termes d'efficacité, de rentabilité et de sécurité.

Le **Réalisateur** est la personne chargée des actions prévues (au sens de RACI).

Spécifier le périmètre d'un processus

Un processus / une catégorie de processus peuvent être reliés à différents types d'objets.

Une page spécifique pour chaque type d'objet est proposée dans les propriétés :

- **Risques** : risques qui portent sur le processus.

  Pour plus de détails, voir Gérer les risques.
- **Contrôles** : contrôles qui portent sur le processus.

  Pour plus de détails, voir Gérer les contrôles.
- **Incidents**

  Pour plus de détails, voir Collecte des incidents.
- **Plans d'action**

  Pour plus de détails, voir Gérer les plans d'action.

  *Pour visualiser les réglementations qui impactent un processus, dépliez la section **Impact Réglementaire**. Pour plus de détails, voir Gérer la base réglementaire.*

Spécifier les responsabilités

Les responsabilités sur un processus sont assumées par des personnes avec des rôles différents.

Pour spécifier les responsabilités sur un processus :

1. Dans la fenêtre de propriétés d'un processus, dépliez la section **Responsabilités**.
   Vous pouvez ici assignez les responsabilités suivantes :
   - **Autorité**
   - **Consulté**
   - **Informé**

     ☛ *Ces trois premières responsabilités correspondent aux Responsabilités RACI. Voir Les responsabilités (RACI).*

     ☛ *Le **Réalisateur** du processus est à spécifier dans la section **Caractéristiques**.*
   - **Correspondant Risque**

     Le correspondant Risque est responsable de l'évaluation des risques de son périmètre, ainsi que de la mise en œuvre des plans d'action relatifs à ces risques.

     ☛ *Vous pouvez spécifier plusieurs correspondants Risque sur un même processus.*
   - **Correspondant Contrôle**

     Le correspondant Contrôle est responsable de l'évaluation et de l'exécution des contrôles de son périmètre ainsi que de mise en œuvre des plans d'action relatifs à ces contrôles.

     ☛ *Vous pouvez spécifier plusieurs correspondants Contrôle sur un même processus.*

Spécifier les sous-processus

Pour spécifier les sous-catégories d'une catégorie de processus :

1. Dans la fenêtre de propriétés d'une catégorie de processus, dépliez la section **Sous-processus**.
   Vous pouvez spécifier :
   - les composants de la catégorie de processus
   - les processus rattachés

Pour spécifier les sous-processus d'un processus :

1. Dans la fenêtre de propriétés du processus, dépliez la section **Sous-processus et opérations**.
   Vous pouvez spécifier :
   - les sous-processus
   - les opérations rattachées

Gérer la continuité d'activité

☛ *Les fonctionnalités suivantes sont disponibles avec **Hopex BCM** seulement.*

Pour accéder aux (BIA) Bilans d'Impact sur l'Activité et PCA (Plans de Continuité d'Activité) relatifs à un processus / une catégorie de processus :

- Ouvrez les propriétés d'un processus ou d'une catégorie de processus et sélectionnez la page **Continuité d'activité**.

  ☛ *Pour plus de détails, voir :*

  - *Définir un Bilan d'Impact sur l'Activité*
  - *Concevoir un Plan de Continuité d'Activité*

Pour ajouter une catégorie de processus à un système de MCA :

- Dans le menu contextuel d'une catégorie de processus, sélectionnez **Ajouter à un système de MCA**.

  ☛ *Pour plus de détails, voir Gérer les systèmes de MCA.*

Pour créer un Bilan d'Impact sur l'Activité (BIA) à partir d'une catégorie de processus:

- Faites un clic droit sur la catégorie de processus et sélectionnez **Créer un BIA**.

Les autres sections d'un processus

La page de propriétés d'un processus présente les sections suivantes :

- **Objectifs** : voir L'environnement stratégique
- **Actifs informatiques** : des ressources informatiques (applications, bases de données et serveurs) sont mises à la disposition des processus pour sa mise en œuvre.

  ☛ *Voir Gérer les applications.*
- **Entités** : entités qui interviennent dans le cadre du processus.

  ☛ *Voir Gérer les entités.*
- **Lignes métier** : lignes métier qui utilisent les services du processus.

  ☛ *Voir Gérer les lignes métier.*

Gérer les lignes métier

📖 *Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.*

Accéder aux lignes métier

Pour accéder aux lignes métier de l'organisation :

- Dans la barre de navigation, sélectionnez **Environnement > Organisation > Lignes métier**.

A partir de cette page, vous pouvez visualiser sous forme d'arborescence les lignes métier de l'organisation, consulter leurs propriétés et créer de nouveaux objets.

☛ *La liste des lignes métier détenus par une ligne métier est accessible dans la page de propriétés d'une ligne métier, dans la section **Sous-lignes métier**.*

Pour accéder aux caractéristiques d'une ligne métier :

- Dépliez la section **Caractéristiques** de la page de propriétés de la ligne métier qui vous intéresse.

Relier entités et processus à une ligne métier

Une ligne métier peut être mise en œuvre par une entité dans le cadre de processus.

Pour relier une ligne métier à des entités et processus :

- Dans la page de propriétés de la ligne métier, dépliez les sections :
  - **Entités**

    ☛ *Pour plus de détails, voir Gérer les entités.*
  - **Processus**

    ☛ *Pour plus de détails, voir Gérer les catégories de processus et processus.*

Définir les risques et incidents qui impactent la ligne métier

Pour spécifier les risques qui impactent la ligne métier :

- Dans les propriétés de la ligne métier, sélectionnez les pages :
  - **Risques**
  - **Incidents**

Saisir les revenus bruts pour la gestion des incidents

Le bureau **Hopex GRC** permet au gestionnaire des incidents et des pertes de saisir les revenus bruts de l'organisation dans le but d'effectuer une analyse BIA (Approche de l'indicateur de base pour Bâle II).

☛ *Pour plus de détails, voir Revenus bruts.*

Pour spécifier les revenus bruts sur une ligne métier :

1. Dans les propriétés de la ligne métier, sélectionnez la page **Revenus bruts**.
2. Reliez ou créer un produit net bancaire.

Gérer les applications

📖 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

Accéder aux applications

Pour accéder aux applications :

- Dans le bureau **Hopex GRC**, cliquez sur **Environnement > Organisation > Applications**.

Spécifier le périmètre des applications

Vous pouvez par exemple préciser quelle application informatique est mise à la disposition d'une entité ou utilisée lors de l'exécution d'un processus.

Pour visualiser/ modifier la liste des processus supportés ou lignes métier :

- Ouvrez la page de propriétés de l'application et sélectionnez :
  - **Caractéristiques > Processus**, ou
  - **Caractéristiques > Lignes métier**.

Vous pouvez rattacher d'autres types d'objets dans des pages spécifiques des propriétés de l'application :

- **Risques**
- **Contrôles**
- **Plan d'actions**
- **Incidents**
- **Défaillances**

Gérer la continuité d'activité

☛ *Les fonctionnalités suivantes sont disponibles avec **Hopex BCM** seulement.*

Pour accéder aux (BIA) Bilans d'Impact sur l'Activité et PCA (Plans de Continuité d'Activité) relatifs à une application :

- Ouvrez les propriétés d'une application et sélectionnez la page **Continuité d'activité**.

☛ *Pour plus de détails, voir :*

- *Définir un Bilan d'Impact sur l'Activité*
- *Concevoir un Plan de Continuité d'Activité*

Gérer les sites

📖 *Un site est un lieu géographique où est implantée l'entreprise. Les sites peuvent être des sites types tels que le siège, l'agence, l'usine, ou des lieux géographiques précis.*

Accéder aux sites

Pour accéder aux sites :

- Dans le bureau **Hopex GRC**, cliquez sur **Environnement > Organisation > Sites**.

Gérer la continuité d'activité

☛ *Les fonctionnalités suivantes sont disponibles avec **Hopex BCM** seulement.*

Pour accéder aux (BIA) Bilans d'Impact sur l'Activité et PCA (Plans de Continuité d'Activité) relatifs à un site :

- Ouvrez les propriétés d'un site et sélectionnez la page **Continuité d'activité**.

  ☛ *Pour plus de détails, voir :*

  - *Définir un Bilan d'Impact sur l'Activité*
  - *Concevoir un Plan de Continuité d'Activité*

L'ENVIRONNEMENT FINANCIER

Pour accéder aux éléments de l'environnement financier :

❱ Dans l'arbre de navigation, cliquez sur **Environnement > Finances**.

Comptes

Cette arborescence affiche, pour chaque compte, les contrôles qui lui sont associés.

☛ *Ces comptes sont à surveiller dans une optique de conformité SOX.*

Caractéristiques d'un compte

Les caractéristiques des comptes sont les suivantes :

- **Type de compte**
  Le compte de pertes et profits présente un descriptif des charges et produits de l'entreprise au cours de l'exercice comptable en question. Vous pouvez préciser si le compte est de type :
  - "Profits"
  - "Pertes"
- **Valeur totale** : vous pouvez saisir un montant pour ce compte.
  ☛ *Un ordre de grandeur peut suffire.*
- **Statut**
  - "Ouvert" : le compte est actif
  - "Fermé" : le compte est inactif
- **Sous-comptes** : le compte peut être composé de sous-comptes.
- **Entités** et **Processus** : vous pouvez relier le compte à des entités et processus.
- **Eléments financiers** :
  - Perte
  - Gain
  - Récupération
  - Provision

Relier des contrôles à un compte

Pour relier des contrôles à un compte :

1. Dans les propriétés du compte, sélectionnez la page **Contrôles**.
2. Reliez un ou plusieurs contrôles.

Produits

Cette arborescence affiche, pour chaque produit, les incidents non clos qui le concernent.

> 🕮 *Un produit représente un ou plusieurs articles, objets, biens ou services, résultat d'une activité agricole, industrielle ou de service, qui sont proposés par une entreprise.*

Pour créer ou relier des incidents à un produit :

1. Ouvrez les propriétés du produit et sélectionnez la page **Incidents**.
2. Créez ou reliez des incidents.

Vous pouvez visualiser, pour chaque incident :

- son statut
- sa date de déclaration
- l'entité du déclarant
- les pertes associées

Revenus bruts

Les revenus bruts de l'organisation sont saisis par le gestionnaire des incidents et des pertes par ligne métier et servent dans le cadre d'une analyse BIA (Approche de l'indicateur de base, Bâle II).

> ☛ *Pour plus de détails, voir Approche de l'indicateur de base (BIA).*

Pour créer un revenu brut (produit net bancaire) :

1. Cliquez sur **Environnement > Finances > Revenus bruts**.
2. Cliquez sur **Nouveau**.
3. Renseignez les propriétés :
   - **Ligne métier**.
   - **Date de début** et **Date de fin**
   - **Montant de revenu**.

L'ENVIRONNEMENT STRATÉGIQUE

La hiérarchie des objectifs stratégiques de votre organisation est affichée dans une arborescence.

> 🕮 *Un objectif est un but que l'on cherche à atteindre ou la cible visée pour un processus ou une opération. Il permet de mettre en évidence les points que l'on veut améliorer pour ce processus ou cette opération.*

Pour accéder à la hiérarchie des objectifs de votre organisation :

- Dans l'arbre de navigation, sélectionnez **Environnement > Organisation > Objectifs**.

Pour créer un objectif :

- Cliquez sur le bouton **Nouveau**.

Selon la solution dont vous disposez, les informations suivantes sont affichées :

- (**Hopex Internal Control**) le nombre des contrôles contribuant à la réalisation de chaque objectif .
- (**Hopex Enterprise Risk Management**) le nombre de risques susceptibles de constituer une entrave à la réalisation de l'objectif.

L'ENVIRONNEMENT DES RISQUES

Pour analyser un risque, il est nécessaire de prendre en compte tous les éléments de son environnement.

Décrire l'environnement des risques

Pour décrire les objets pouvant constituer l'environnement d'un risque :

❱ Dans le bureau **Hopex GRC**, cliquez sur **Environnement > Risques**.

☛ *Les types de risques sont à définir dans **Risques > Par Type de risque**.*

Vous pouvez ici définir :

- les facteurs de risque

  🕮 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.*

- les conséquences de risque

  🕮 *Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.*

Définir l'environnement d'un risque donné

Pour définir l'environnement d'un risque :

1. Dans la page **Caractéristiques** de la fenêtre de propriétés d'un risque, dépliez la section **Analyse**.
   Un risque est caractérisé par des :
   - **Types de risque**

     🕮 *Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.*

   - **Facteurs de risque**

     🕮 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté*

technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.

- **Conséquences de risques**

  Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.

- **Risques associés**

Les types de risque

Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.

Un type de risque permet de caractériser un risque. Un risque peut par exemple être de type réglementaire, juridique, technique, etc.

Créer un type de risque

Pour créer vos propres types de risque :

1. Dans la barre de navigation, cliquez sur **Riques > Par type de risque**.
2. Cliquez sur **Nouveau**.
3. Renseignez le nom du type de risque et cliquez sur **OK**.
   Le nouveau type de risque apparaît dans l'arborescence du navigateur.

   ☛ *Vous pouvez de la même manière créer un sous-type de risque à partir d'un type de risque.*

Analyser les impacts d'un type de risque

Un rapport vous permet d'analyser les impacts d'un type de risque. Voir Décomposition des impacts d'un type de risque.

Les facteurs de risque

Nombreux de facteurs de risque sont définis dans le cadre de réglementations internationales, nationales ou inter-professionnelles, ou au sein de l'entreprise elle-même.

Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.

Il est possible d'associer à chaque risque un ou plusieurs facteurs de risque, sources de risques ou dangers qui ont intrinsèquement le potentiel de mettre en danger le fonctionnement de l'organisation. Par exemple, des produits chimiques dangereux, des concurrents, des gouvernements, etc.

Les conséquences des risques

Pour définir les conséquences associées à un risque :

- Dans la page d'un risque, section **Analyse**, onglet **Conséquences de risque**, cliquez sur l'onglet **Nouveau**.
  La page de création d'une conséquence apparaît.

  ☛ *Une conséquence de risque ne pouvant porter que sur un seul risque, le champ **Risque** est pré-rempli avec le risque courant.*

La conséquence créée apparaît dans la liste des conséquences associées au risque.

L'ENVIRONNEMENT DES CONTRÔLES

Pour décrire l'environnement des contrôles et accéder aux sous-types de contrôle :

- Dans la barre de navigation, cliquez sur **Contrôles > Par type de contrôle**.

  Un type de contrôle permet de classifier les contrôles mis en oeuvre dans l'entreprise conformément à des standards sectoriels ou réglementaires (Cobit, etc.).

Pour visualiser les sous-types de contrôle et contrôles :

- Cliquez sur le signe + du type de contrôle qui vous intéresse.
  Pour chaque type de contrôle, le nombre de contrôles de premier niveau est affiché.

Pour enlever et/ou relier des contrôles de/à un type de contrôle :

- Ouvrez la page de propriétés du type de contrôle et sélectionnez la page **Contrôles**.

L'ENVIRONNEMENT DE CONFORMITÉ

Hopex GRC vous permet de gérer l'environnement réglementaire de votre organisation ainsi que ses politiques internes.

Pour gérer votre environnement de conformité dans **Hopex** :

- Dans la barre de navigation, sélectionnez **Conformité > Réglementations**.

Vous pouvez :

- importer du contenu UCF à partir d'une liste partagée (Shared List)du Common Controls Hub et définir les articles qui s'appliquent à votre organisation
- créer manuellement des textes de référence, articles et obligations

  Un texte de référence est un texte qui entre dans l'une des catégories suivantes : réglementations (textes de lois qui peuvent entraîner des pénalités s'ils ne sont pas respectés), standards ou normes.

  Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.

  Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.
- créer manuellement des cadres de politique d'entreprise et politiques d'entreprise.

  Un cadre de politique d'entreprise constitue un ensemble de politiques d'entreprise. Les cadres de politique d'entreprise peuvent contenir des sections.

Gérer votre environnement réglementaire

Utiliser l'import UCF

Exigences préalables à l'import UCF

Les directeurs du contrôle interne ou les Managers GRC peuvent télécharger du contenu UCF ("Authority Documents", "Citations" et "Common Controls" et le mettre à jour.

Pour pouvoir importer ce contenu dans **HOPEX UCF**, vous devez avoir :

- **Hopex GRC** (ou **Hopex Internal Control** au minimum) ET **HOPEX UCF**
- un compte UCF et une clé API UCF
- une "Shared List" (liste partagée) avec les (seuls) "Authority Documents" que vous voulez importer.

  ☛ *Pour plus de détails, voir Unified Compliance Framework.*

- paramétré les options UCF dans **HOPEX UCF**

  ☛ *Dans le Common Controls Framework d'UCF, les informations sont généralement disponibles en anglais.*

  *Si vous souhaitez utiliser **HOPEX UCF** alors que vous utilisez **Hopex** dans une langue de données utilisateur autre que l'anglais, vous devez :*

  - *paramétrer la langue de données souhaitée (par exemple, le français, si vous souhaitez utiliser **Hopex** avec des données en français)*
  - *procéder à l'import*
  - *répéter l'opération (changer de langue de données + procéder à l'import) autant de fois que de langues souhaitées*

Paramétrer l'import UCF

Pour paramétrer l'import UCF :

1. Dans **Menu principal**, sélectionnez **Paramètres > Options**.
2. Dans la fenêtre d'options, dépliez **Echange de données > Import > Intégration UCF Common Controls Hub**.
3. Sélectionnez la case **Activer l'import UCF**.
4. Saisissez l'URL correspondant à l'API UCF.

   ```
   https://api.unifiedcompliance.com/
   ```

5. Saisissez votre **Clé d'authentification** pour l'API UCF.

   ☛ *Pour récupérer votre clé d'authentification dans votre espace de travail Unified Compliance Framework :*

   - *Cliquez sur Settings > API Manager > API Keys.*
   - *Cliquez sur "Create Credentials" et copiez-collez votre clé API.*

6. Cliquez sur **OK**.

Importer des données à partir du Common Controls Hub

Les responsables de la conformité doivent créer les éléments de l'environnement UCF dans Compliance **HOPEX UCF**. Il s'agit de :

- importer les données pertinentes à partir du Common Controls Hub d'UCF (Authority Documents, Citations et Controls)
- déclarer les articles appropriés comme étant pertinents pour votre organisation : voir Définir les réglementations et politiques internes applicables.

Pour importer les données UCF :

1. Dans l'arbre de navigation, sélectionnez **Environnement > Conformité > Textes de référence**.
2. Cliquez sur **Importer du contenu UCF**.
3. Cliquez sur **Suivant.**
4. Sélectionnez la "Shared List" de votre Common Controls Hub.
5. Cliquez sur **Suivant**.

6. Sélectionnez le(s) "Authority Document(s)" que vous voulez importer dans **Hopex**.

> ☛ *Si vous mettez à jour un "Authority Document" déjà importé, il peut être utile de comparer les colonnes **Dernier import de mise à jour UCF** et **Dernière mise à jour UCF disponible**.*

7. Cliquez sur **Suivant**.

> ☛ *Une fois que les données UCF ont été importées dans **Hopex**, il n'est pas possible de les exporter (pour les transférer vers un autre référentiel par exemple).*

Créer manuellement votre contenu réglementaire

Créer des textes de référence et leur contenu

Si vous n'utilisez pas l'import UCF, vous pouvez créer votre propre contenu réglementaire.

> ☛ *Le contenu réglementaire que vous créez manuellement est considéré applicable par défaut.*

Pour créer un texte de référence :

1. Dans la barre de navigation, cliquez sur **Conformité > Réglementations > Textes de référence**.
2. Cliquez sur **Nouveau**.

> 🕮 *Un texte de référence est un texte qui entre dans l'une des catégories suivantes : réglementations (textes de lois qui peuvent entraîner des pénalités s'ils ne sont pas respectés), standards ou normes.*

Pour créer le contenu de votre texte de référence :

1. Dans la barre de navigation, cliquez sur **Conformité > Réglementations > Textes de référence**.
2. Faites un clic droit sur un texte de référence et sélectionnez :
   - **Nouveau > Section de texte de référence**

     > 🕮 *Une section est une citation d'un texte de référence, qui n'est associée à aucune obligation légale et qui contient d'autres sections ou articles.*

   - **Nouveau > Article de texte de référence**

     > 🕮 *Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.*

Créer des obligations

Pour créer des obligations :

1. Dans la barre de navigation, cliquez sur **Environnement > Conformité > Obligations**.
2. Faites un clic droit sur la racine de l'arborescence et sélectionnez **Nouveau > Obligation**.

> 🕮 *Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.*

Gérer vos politiques internes

Hopex GRC vous permet de gérer les politiques internes à votre entreprise au même titre que les réglementations.

Vous pouvez créer des cadres de politiques d'entreprise ainsi que leur contenu (politiques d'entreprise).

> 🕮 *Un cadre de politique d'entreprise constitue un ensemble de politiques d'entreprise. Les cadres de politique d'entreprise peuvent contenir des sections.*

Pour créer un cadre de politiques d'entreprise :

1. Dans l'arbre de navigation, cliquez sur **Conformité > Réglementations > Cadres de politiques d'entreprise**.
2. Cliquez sur **Nouveau**.

Pour créer le contenu de votre cadre de politiques d'entreprise :

3. Faites un clic droit sur le cadre de politiques d'entreprise que vous venez de créer et sélectionnez :
   - **Nouveau > Section de cadre de politique d'entreprise**
   - **Nouveau > Politique d'entreprise**

Définir les réglementations et politiques internes applicables

Applicabilité du contenu réglementaire

Si vous avez procédé à un import UCF, vous devez définir le contenu réglementaire applicable à votre organisation. En effet, tous les articles/sections d'un texte de référence ne vous sont pas applicables.

> ☛ *Le contenu réglementaire que vous avez créé manuellement s'applique automatiquement à votre organisation.*

Les responsables de la conformité doivent étudier les textes de référence importés, identifier le contenu applicable et le déclarer comme tel. Seul le contenu considéré applicable sera visible des parties prenantes dans les registres **Hopex**. Voir Gérer le registre de conformité.

Procéder à la revue des textes de référence après import

Une fois que les données UCF ont été importées, une arborescence apparaît dans le menu **Environnement**, visible par les profils de type "Manager".

Cette arborescence affiche :

- les textes de référence (Authority Documents),
- les articles (Citations)
- les obligations légales rattachées (Common Controls).

Elle se base sur les relations entre obligations impactées / contributrices (supported/supporting) telles que définies dans UCF.

Vous pouvez, à partir de cette arborescence :

- procéder à la revue des textes de référence importés.
- spécifier le contenu pertinent pour votre organisation.

Sélectionner le contenu réglementaire applicable à votre organisation

☛ *Le contenu réglementaire que vous avez créé manuellement est automatiquement considéré comme applicable.*

Pour spécifier le contenu applicable :

1. Dans la barre de navigation, sélectionnez **Conformité > Textes de référence**.
2. Dépliez l'arborescence et sélectionnez la case correspondant aux textes de référence / articles / sections auxquels vous devez vous conformer.

☛ *Le cadre grisé*  *indique que seuls certains éléments du contenu ont été sélectionnés dans l'arborescence.*

Définir le périmètre des réglementations et politiques internes

Vous pouvez définir le périmètre de vos textes de référence et cadres de politiques d'entreprise, c'est-à-dire définir les éléments sujets.

Pour cela :

1. Dans la barre de navigation, sélectionnez :
   - **Conformité > Réglementations > Textes de référence**, ou
   - **Conformité > Réglementations > Cadres de politiques d'entreprise**.
2. Dans les propriétés d'un élément de contenu réglementaire ou de politique interne, dépliez la section **Éléments Sujets**.
3. Reliez des entités, applications ou processus.

LES RESPONSABILITÉS (RACI)

Les solutions **Hopex** permettent de définir les responsabilités des personnes sur certains objets via la matrice RACI.

☛ *RACI est l'acronyme de Responsible (Réalisateur), Accountable (Autorité), Consulted (Consulté), Informed (Informé).*

Niveaux de responsabilité

Les niveaux de responsabilité proposés sont les suivants :

Responsabilité	Explication
Réalisateur	Personne chargée de la réalisation des actions prévues.
Autorité	Personne rendant compte de l'avancement des actions prévues et prenant des décisions. Il n'y a qu'une seule "Autorité" par action.
Consulté	Personne consultée prioritairement avant une action ou décision.
Informé	Personne devant être informée après une action ou décision.

Hopex permet de préciser le niveau de responsabilité de différentes personnes :

- sur une catégorie de processus ou un processus
- sur un risque
- sur un contrôle

Spécifier les responsabilités

La responsabilité du pilotage d'un objet peut être assumée par une ou plusieurs personnes.

Pour préciser les personnes concernées par un objet :

1. Dans la page de propriétés de l'objet, dépliez la section **Responsabilités**.
2. Créez des assignations de responsabilité dans l'un des onglets suivants :
   - **Réalisateur**
   - **Autorité**
   - **Consulté**
   - **Informé**.

INDICATEURS CLÉS

Un indicateur clé est une métrique utilisée par l'organisation pour alerter en cas d'exposition croissante à des risques dans différents secteurs de l'entreprise.

Les indicateurs clés vous permettent de surveiller les valeurs d'indicateurs (qu'ils soient saisis manuellement dans **Hopex** ou importés de manière automatisés). Vous pouvez ainsi gérer des KPI (indicateurs clés de performance) ou des indicateurs de contrôle.

Pour administrer les indicateurs clés, voir Administrer les indicateurs clés.

☛ *Les indicateurs clés sont disponibles avec **Hopex Internal Control** et **Hopex Enterprise Risk Management**.*

- ✓ Accéder aux indicateurs clés
- ✓ Définir des indicateurs clés
- ✓ Catégories d'indicateurs clés
- ✓ Détailler les indicateurs clés
- ✓ Vue d'ensemble des indicateurs clés
- ✓ Définir la fréquence des mesures et les notifications
- ✓ Visualiser le graphique d'indicateur
- ✓ Saisir des valeurs périodiques d'indicateurs clés

ACCÉDER AUX INDICATEURS CLÉS

Pour accéder aux indicateurs clés à partir d'une liste :

1. Dans la barre de navigation, sélectionnez **Environnement > Indicateurs**.
   Vous obtenez la liste de tous les indicateurs de votre environnement.

Les informations suivantes apparaissent en colonne pour chaque indicateur :

- Statut courant
- Dernière mesure (en jours)
- Temps avant défaillance (en jours)

  📖 *Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".*
- Valeur
- Limite basse
- Limite haute
- Entités

  ☛ *Pour plus d'informations sur les informations disponibles en colonne, voir Définir des indicateurs clés.*

DÉFINIR DES INDICATEURS CLÉS

Créer un indicateur clé

Pour créer un indicateur clé :

1. Dans la barre de navigation, sélectionnez **Environnement > Indicateurs**.
2. Cliquez sur **Nouveau**.
   Une fenêtre de création apparaît.

   ☛ *Vous pouvez également créer un indicateur clé depuis la page d'accueil (zone d'**Accès rapide > Actions > Créer un indicateur clé**).*
3. Définissez une **Limite basse** et **Limite haute**.
4. Spécifiez la **Catégorie** de l'indicateur.
   La catégorie de l'indicateur détermine la façon dont les valeurs d'indicateurs sont interprétées et le statut de l'indicateur.
   - **Standard**: la limite haute représente l'objectif.
   - **Inversé** : inverse de « Standard »
   - **Valeurs acceptées** : Toutes les valeurs à l'intérieur des limites sont acceptées.
   - **Valeurs exclues** : l'ensemble des valeurs à l'intérieur des limites définies sont rejetées.

   ☛ *Si plusieurs algorithmes sont disponibles pour une même catégorie d'indicateur, le champ **Logique d'interprétation d'indicateur clé** est proposé. Vous pouvez sélectionner un algorithme pour calculer les statuts de l'indicateur. Pour plus de détails, voir Lien entre catégorie d'indicateur clé et logique d'interprétation.*
5. Indiquez si vous avez besoin d'agréger les valeurs sur une période de temps définie.
   L'agrégation n'est pas sélectionnée par défaut.

   ☛ *Si vous souhaitez agréger les valeurs, voir Spécifier la période et la méthode d'agrégation.*
6. Cliquez sur **OK** pour créer votre indicateur.

   ☛ *Vous ne pouvez pas changer de catégorie d'indicateur clé, de période d'agrégation ou de méthode d'agrégation après création de l'indicateur clé.*

Spécifier la période et la méthode d'agrégation

Les valeurs d'indicateurs ne sont pas agrégées par défaut. Vous devez indiquer spécifiquement que les valeurs sont à agréger.

Pour agréger les valeurs :

1. Dans l'assistant de création de l'indicateur clé, dé-sélectionnez la case **Ne pas agréger les valeurs d'indicateurs clés**.
   Deux champs supplémentaires apparaissent dans l'assistant :

2. Spécifiez la **Période d'agrégation**.

   📖 *La période d'agrégation est la période au cours de laquelle les valeurs de l'indicateur clé sont agrégées, de manière à calculer sa valeur et son statut.*

   - Annuelle
   - Semestrielle
   - Trimestrielle
   - Mensuelle
   - Bimensuelle
   - Hebdomadaire

3. Spécifiez la **Méthode d'agrégation**.

   📖 *Une méthode d'agrégation est une opération mathématique réalisée sur les valeurs agrégées de l'indicateur clé, de manière à calculer la valeur de ce dernier ainsi que son statut.*

   - Somme
   - Moyenne

   ☛ *Veuillez noter que l'administrateur fonctionnel peut créer des périodes et méthodes d'agrégation.*

   ☛ *Une fois l'indicateur clé créé, il n'est plus possible de spécifier une autre période d'agrégation ou une autre méthode d'agrégation.*

Exemple d'indicateur clé

📖 *Un indicateur clé est une métrique utilisée par l'organisation pour alerter en cas d'exposition croissante à des risques dans différents secteurs de l'entreprise.*

Ci-dessous un exemple d'indicateur clé. Il illustre la façon dont les indicateurs clés sont utilisés ainsi que leurs caractéristiques.

Un indicateur clé vise à surveiller le chiffre d'affaires d'une entité juridique. L'objectif est fixé à 12 millions (d'euros).

L'indicateur clé mesure le chiffre d'affaires mensuel pour pouvoir prendre des mesures appropriées si nécessaire.

Le chiffre d'affaires mensuel doit toujours se situer entre 900k et 1,1 million d'euros. La valeur de l'indicateur clé est mesurée deux fois par mois, ce qui signifie que les valeurs de l'indicateur clé saisies chaque mois sont additionnées de manière à obtenir le chiffre d'affaires mensuel.

Dans cet exemple les différentes caractéristiques décrites dans **Hopex** sont :

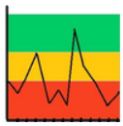
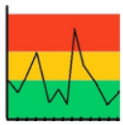
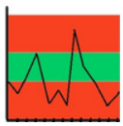
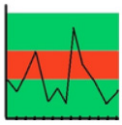
- **Limite basse** 900k
- **Limite haute** 1100k
- **Catégorie**: Standard (toutes les valeurs au-dessus de la limite haute sont considérées satisfaisantes)
- **Période d'agrégation**: mensuelle
- **Méthode d'agrégation**: somme
- **Statuts** pour le chiffre d'affaires mensuel :

Satisfaisant	>= 1050
Acceptable (avec avertissement)	>= 975 et < 1050
Insatisfaisant	>= 925 et < 975
Critique	>= 900 et < 925
Non Acceptable	< 900

CATÉGORIES D'INDICATEURS CLÉS

La catégorie d'indicateur clé détermine la façon dont les valeurs de l'indicateur sont interprétées, de façon à obtenir le statut de l'indicateur et le temps avant défaillance.

Description des catégories d'indicateurs clés

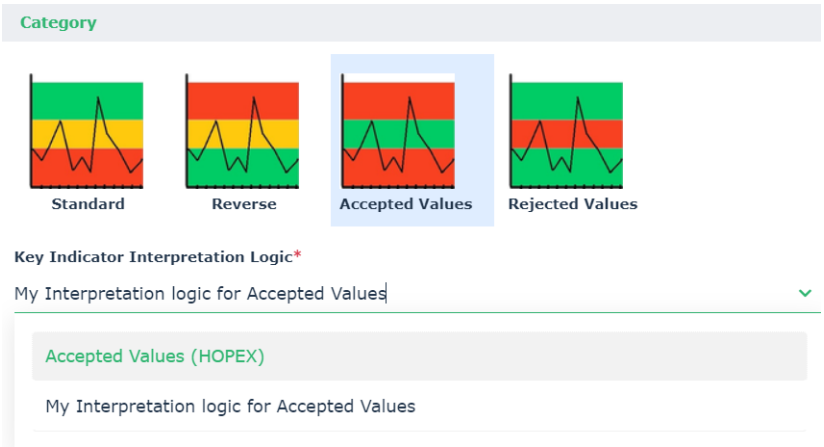
Catégorie d'indicateur clé	Signification	Représentation visuelle
Standard	La limite haute représente l'objectif. Pour les valeurs au-dessus de la limite supérieure, l'indicateur clé est jugé satisfaisant (en vert).	
Inversé	Inverse de « Standard » Toutes les valeurs au-delà de la limite haute sont rejetées Plus la valeur est basse, mieux c'est.	
Valeurs acceptées	Toutes les valeurs à l'intérieur des limites sont acceptées.	
Valeurs exclues	Toutes les valeurs à l'intérieur des limites sont rejetées.	

Lien entre catégorie d'indicateur clé et logique d'interprétation

Une catégorie d'indicateur clé est reliée à une logique d'interprétation qui utilise un algorithme pour calculer le statut de l'indicateur clé. Plusieurs logiques d'interprétation peuvent être associées à une catégorie d'indicateur clé. Il est ainsi possible de proposer plusieurs façons de calculer le statut pour une catégorie d'indicateur clé.

Si plusieurs logiques d'interprétation sont disponibles pour une catégorie d'indicateur clé, les logiques d'interprétation sont proposées au moment de la création de l'indicateur clé.

Si, par exemple, plusieurs logiques d'interprétation existent pour la catégorie « Valeurs acceptées », le champ suivant apparaît :



☛ *Les logiques d'interprétation d'indicateur clé peuvent être créées par votre administrateur fonctionnel.*

DÉTAILLER LES INDICATEURS CLÉS

Après avoir créé votre indicateur, vous pouvez modifier certaines de ses caractéristiques et le décrire de manière plus détaillée.

> ☛ *Vous ne pouvez pas changer de catégorie d'indicateur clé, de période d'agrégation ou de méthode d'agrégation après création de l'indicateur clé.*

Modifier les paramètres d'un indicateur clé

Une fois que l'indicateur clé a été créé, vous ne pouvez plus modifier la catégorie de l'indicateur, la période d'agrégation ou la méthode d'agrégation. Vous pouvez cependant modifier certains paramètres.

Pour modifier les paramètres :

1. Voir Accéder aux indicateurs clés.
2. Dans la page **Caractéristiques** des propriétés de l'indicateur, dépliez la section **Avancé**.
3. Cliquez sur **Modifier les paramètres**.
   Dans la fenêtre qui apparaît, vous pouvez modifier :
   - la **Limite Haute** et la **Limite Basse**.
   - le **Nombre de valeurs utilisées pour le calcul du Temps avant défaillance**

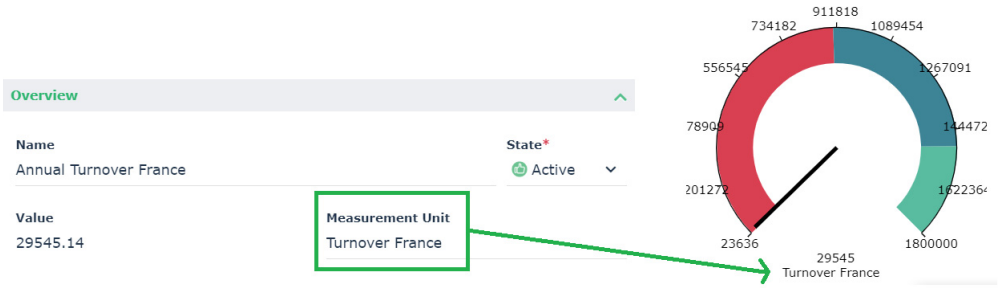
     > 🕮 *Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".*
     >
     > ☛ *Le **Nombre de valeurs utilisées pour le calcul du Temps avant défaillance** correspond au nombre de valeurs passées à prendre en compte. Il s'agit de 12 valeurs par défaut. Plus la valeur est élevée meilleur est la résultat mais les performances peuvent être amoindries. Il est donc important de trouver le juste équilibre.*

Lorsque vous modifiez ces paramètres, le Statut et le Temps avant défaillance sont automatiquement mis à jour.

Définir une unité de mesure à afficher dans les rapports

Dans la page de propriétés d'un indicateur clé, le champ **Unité de Mesure** représente ce que l'indicateur met sous surveillance. Le contenu du champ est

utilisé pour servir de légende à l'axe des ordonnées dans les graphiques et rapports d'indicateurs.



Pour plus de détails sur les graphiques et rapports, voir Visualiser le graphique d'indicateur.

Activer / désactiver un indicateur clé

un indicateur clé est activé par défaut au moment de sa création. Vous pouvez être amené à le désactiver s'il attend sa fin de vie ou si aucune autre mesure n'est réalisée. Vous pouvez désactiver un indicateur clé en modifiant son état.

Pour désactiver un indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Ouvrez la page de propriétés de l'indicateur clé.
3. Dans le champ **Etat**, sélectionnez "Inactif".

Si vous passez l'état à « Inactif » :

- La valeur et le statut de l'indicateur clé sont calculés une dernière fois.
- Il n'est plus possible de saisir de nouvelles valeurs.
- Toutes les notifications existantes sont désactivées.

> ☛ *Pour pouvoir saisir de nouvelles valeurs, et/ou pour modifier les propriétés d'un indicateur clé, passez son état à « Actif ».*
>
> ☛ *Il convient de distinguer l'état de l'indicateur clé de son statut.*

Spécifier le périmètre de l'indicateur clé

Pour spécifier le périmètre de l'indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Dans les pages de propriétés de l'indicateur clé, sélectionnez la page **Caractéristiques** et dépliez la section **Périmètre**.

Vous pouvez spécifier ici les objets associés :

- entités

  📖 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.*

- catégories de processus

  📖 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

- processus

  📖 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

- applications

Pour relier des indicateurs clés à une entité :

1. Dans la page de propriétés d'un indicateur clé, dépliez la section **Périmètre** puis sélectionnez l'onglet **Entités**.
2. Déliez l'entité appropriée.

Créer des plans d'action

Pour définir des plans d'action sur un indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés de l'indicateur clé, sélectionnez la page **Plans d'action**.
3. Reliez un plan d'action existant ou créez-en un.

   📖 *Un plan d'action est constitué d'une série d'actions, avec pour objectif de réduire les risques et les événements ayant un impact négatif sur l'activité de l'entreprise.*

   ☛ *Pour plus de détails sur les plans d'action, voir la section correspondante dans la rubrique « Fonctionnalités communes » de la documentation en ligne.*

Relier des risques

Pour relier des risques à un indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Dans les pages de propriétés de l'indicateur clé, sélectionnez la page **Caractéristiques** et dépliez la section **Risques**.
3. Reliez un risque existant ou créez-en un.

VUE D'ENSEMBLE DES INDICATEURS CLÉS

> ☛ *Voir Accéder aux indicateurs clés.*

La page de propriétés **Vue d'ensemble** donne accès à:

- une carte de l'indicateur clé, qui fournit un aperçu de ses principales caractéristiques.

  > ☛ *Pour plus de détails sur les cartes d'objets, voir Carte d'un objet, dans la section "Plateforme - Fonctionnalités communes".*

- des informations calculées, sous forme de tableau de bord

Statut de l'indicateur clé

Statuts par défaut

Les statuts suivants sont disponibles par défaut :

- Non connu
- Satisfaisant
- Acceptable (avec avertissement)
- Insatisfaisant
- Critique
- Non acceptable

La signification des statuts dépend de la catégorie de l'indicateur clé et de la logique d'interprétation associée à cette catégorie.

> ☛ *Le statut de l'indicateur clé est à distinguer de l'état (qui permet d'indiquer si l'indicateur clé est actif ou inactif).*

Le statut de l'indicateur clé permet d'émettre un avertissement lorsque cela se révèle nécessaire. Pour plus de détails, voir Définir la fréquence des mesures et les notifications.

Informations concernant le calcul du statut de l'indicateur clé

Le statut de l'indicateur clé se base sur :

- les dernières valeurs de l'indicateur clé

  ☛ *Pour plus de détails sur les valeurs de l'indicateur clé, voir Saisir des valeurs périodiques d'indicateurs clés*

- la période d'agrégation

  🕮 *La période d'agrégation est la période au cours de laquelle les valeurs de l'indicateur clé sont agrégées, de manière à calculer sa valeur et son statut.*

- la méthode d'agrégation

  🕮 *Une méthode d'agrégation est une opération mathématique réalisée sur les valeurs agrégées de l'indicateur clé, de manière à calculer la valeur de ce dernier ainsi que son statut.*

  ☛ *Pour plus de détails, voir Spécifier la période et la méthode d'agrégation.*

Le statut de l'indicateur clé est calculé lorsque :

- une nouvelle valeur est créée

  ☛ *Pour plus de détails, voir Saisir des valeurs périodiques d'indicateurs clés.*

- une valeur existante est supprimée
- les limites de l'indicateur clé sont modifiées
- l'état de l'indicateur (actif ou inactif) a été modifié

  ☛ *Pour plus de détails, voir Activer / désactiver un indicateur clé.*

Temps avant défaillance

Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".

Une interpolation linéaire des dernières valeurs est réalisée pour calculer le temps avant défaillance.

Vous devez spécifier le nombre de valeurs passées à prendre en compte pour le calcul du temps avant défaillance. Pour plus de détails, voir Vue d'ensemble des indicateurs clés.

Valeur	Détails
Non connu	Quantité de données disponibles insuffisante (il est nécessaire d'avoir au moins deux valeurs agrégées)
Non prévisible	Les valeurs de l'indicateur évoluent de telle manière qu'il est impossible de prévoir le statut « Non acceptable ». ☛ *9999 est affiché dans la colonne Temps avant défaillance de la liste des indicateurs clés.*
0 jour	L'indicateur clé se trouve déjà dans le statut « Non acceptable ».

Dernière mesure de l'indicateur clé

Dernière mesure indique le temps écoulé (en nombre de jours) depuis que la dernière valeur de l'indicateur clé a été saisie.

Cette valeur est arrondie à l'entier le plus proche.

Valeur de l'indicateur clé

Vous pouvez également visualiser la valeur de l'indicateur dans la carte d'identification de l'indicateur clé.

La valeur de l'indicateur correspond à la dernière mesure agrégée de l'indicateur clé.

☛ *Si aucune période ou aucune méthode d'agrégation n'a été définie, la valeur correspond à la dernière mesure de l'indicateur clé.*

Voir également : Saisir des valeurs périodiques d'indicateurs clés.

DÉFINIR LA FRÉQUENCE DES MESURES ET LES NOTIFICATIONS

Spécifier la fréquence de mesure

Pour spécifier la fréquence de mesure d'un indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés d'un indicateur clé, sélectionnez la page **Valeurs**.
3. Dans la section **Paramètres des mesures**, sélectionnez un calendrier de pilotage (champ **Fréquence de la mesure**).
   - Fréquence de mesure **quotidienne**
   - Fréquence de mesure **mensuelle**
   - Fréquence de mesure **hebdomadaire**

Le calendrier de pilotage est utilisé pour envoyer des notifications aux utilisateurs appropriés.

Gérer les notifications

Hopex GRC permet d'envoyer des notifications automatiques en se basant sur :

- le statut de l'indicateur clé
- la date de la dernière mesure
- la valeur du temps avant défaillance (nombre de jours)

Vous pouvez de cette manière vous assurer que les propriétaires des indicateurs concernés gèrent les indicateurs de manière adéquate.

Pour spécifier ou modifier les notifications utilisateurs :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés d'un indicateur clé, sélectionnez la page **Notifications**.

Vous pouvez choisir d'envoyer des notifications périodiques :

- à une personne en particulier.

  ☛ *Par défaut, c'est le propriétaire de l'indicateur clé qui reçoit la notification. Vous pouvez ici spécifier une autre personne.*

  ☛ *Les notifications envoyées à des utilisateurs appropriés invitent ces utilisateurs de saisir des valeurs pour l'indicateur clé dont ils ont la charge. Pour plus de détails, voir Saisir des valeurs périodiques d'indicateurs clés.*

- à un ensemble d'utilisateurs (lorsque l'indicateur clé atteint un statut particulier ou lorsque la dernière mesure date de plus d'un certain nombre de jours).

Saisir des valeurs périodiques d'indicateurs clés

Hopex GRC permet au propriétaire de l'indicateur clé ou aux autres personnes autorisées de saisir manuellement une valeur d'indicateur clé, de manière à « alimenter » l'indicateur clé.

Il est également possible d'alimenter automatiquement l'indicateur clé en valeurs.

Saisir manuellement une valeur d'indicateur clé

Pour saisir une valeur d'indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés d'un indicateur clé, sélectionnez la page **Valeurs**.
3. Dépliez la section **Valeurs**, et cliquez sur **Nouveau** pour saisir une valeur.
4. Modifiez la date par défaut si nécessaire.
5. Cliquez sur **OK**.

> ☛ *Il est utile de paramétrer des notifications de manière à être invité périodiquement à saisir des valeurs. Pour plus de détails, voir Gérer les notifications.*

Les valeurs saisies périodiquement permettent d'obtenir la valeur indiquée dans la page **Caractéristiques** de l'indicateur clé.

Paramétrer la saisie automatique de valeurs

Vous pouvez également décider d'alimenter automatiquement l'indicateur clé à intervalles réguliers.

Pour cela :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés d'un indicateur clé, sélectionnez la page **Valeurs**.
3. Dans la section **Paramètres des mesures**, sélectionnez la **Fréquence de la mesure** via un calendrier de pilotage.
4. Sélectionnez la **Logique de calcul de la valeur d'indicateur**

   > ☛ *Pour plus de détails, voir Définir les logiques de calcul des valeurs d'indicateurs clés.*
5. (optionnel) Si la logique de calcul sélectionnée requiert des paramètres, spécifiez la requête dans le champ **Paramètres de calcul**.

   ```
   Query =
   ObjectParameter =
   ```

Un bouton vous permet de **Tester le calcul**.

VISUALISER LE GRAPHIQUE D'INDICATEUR

Hopex GRC permet d'afficher un graphique pour un indicateur spécifique.

Pour accéder à ce graphique :

1. Voir Accéder aux indicateurs clés.
2. Dans les propriétés de l'indicateur clé, sélectionnez la page **Graphique d'indicateur**.

> ☛ *Ce graphique est également disponible dans la page **Vue d'ensemble** des propriétés de l'indicateur.*

Les valeurs de l'indicateur clé sont affichées dans un tableau en-dessous du graphique.

> ☛ *Pour afficher une légende au niveau de l'axe des ordonnées du graphique, voir Définir une unité de mesure à afficher dans les rapports.*

Hopex GRC propose également des rapports permettant de visualiser différents indicateurs. Voir Rapports d'indicateurs clés.

CAMPAGNES D'ÉVALUATION

Les solutions GRC (Governance, Risk & Compliance) permettent d'évaluer les contrôles et les risques par l'intermédiaire de campagnes d'évaluation.

- ✓ Accéder aux évaluations par profil
- ✓ Accéder aux modèles d'évaluation
- ✓ Préparer l'environnement de l'évaluation
- ✓ Lancer une campagne d'évaluation

Voir aussi :

- Suivre l'avancement de l'évaluation
- Gérer les questionnaires

ACCÉDER AUX ÉVALUATIONS PAR PROFIL

Vous pouvez accéder aux fonctionnalités de campagnes d'évaluation à partir de divers profils et bureaux :

Profil	Action	Bureau
Administrateur fonctionnel GRC	- Assigner les rôles aux personnes de l'entreprise. - Définir l'organisation (entités, processus,...) - Déterminer les répondants (qui sont les évaluateurs des risques pour chaque entité)	Bureau Hopex GRC
Manager GRC (Contrôleur interne)	- Création des campagnes d'évaluation - Création des sessions d'évaluation - Suivi des sessions d'évaluation	Bureau Hopex GRC
Contributeur GRC	- Accepter ou refuser un questionnaire - Répondre aux questionnairex	Bureau Contributeur GRC

ACCÉDER AUX MODÈLES D'ÉVALUATION

☛ *Pour accéder aux modèles d'évaluation, vous devez vous connecter en tant qu'Administrateur fonctionnel GRC.*

Pour accéder aux modèles d'évaluation :

1. Dans la barre de navigation, cliquez sur **Administration > Évaluation > Modèles d'évaluation**.
   Les modèles d'évaluation apparaissent.

Les modèle d'évaluation utilisent notamment :

- des caractéristiques évaluées

  🕮 *Une caractéristique évaluée définit ce que l'évaluation cherche à évaluer. Elle peut être associée à une MetaClasse et précisément à l'un de ses MetaAttributs, par exemple : Metaclasse Risque, MetaAttribut: Criticité.*

- un modèle de questionnaire

  🕮 *Un modèle de questionnaire représente la définition du contenu d'un questionnaire.*

  ☛ *Le modèle d'évaluation définit le périmètre de l'évaluation, le modèle de questionnaire à utiliser, éventuellement les schémas d'agrégation à appliquer pour l'interprétation des résultats globaux.*

  Pour plus de détails sur les modèles d'évaluation et leur personnalisation, voir .

PRÉPARER L'ENVIRONNEMENT DE L'ÉVALUATION

Avant de lancer des campagnes d'évaluation, vous devez avoir rempli des pré-requis.

Pré-requis à l'évaluation des risques

Pour l'évaluation des risques, voir Pré-requis à l'évaluation des risques.

Pré-requis à l'évaluation des contrôles

Pour l'évaluation des contrôles, voir les pré-requis dans les sections correspondant aux différents modèles d'évaluation :

- Évaluation des contrôles par entité
- Évaluation des contrôles par entité et texte de référence

LANCER UNE CAMPAGNE D'ÉVALUATION

Créer une campagne d'évaluation

Pour créer une campagne d'évaluation dans **Hopex GRC** :

1. Dans la barre de navigation, cliquez sur **Évaluation > Campagnes**.
2. Cliquez sur **Nouveau**.

   ☛ *Vous pouvez également créer une campagne d'évaluation depuis la page d'accueil (zone d'**Accès rapide > Actions > Créer une campagne d'évaluation**).*
3. Sélectionnez le modèle de questionnaire à utiliser :
   - **Évaluation des risques par entité et processus**
   - **Évaluation des risques par application**

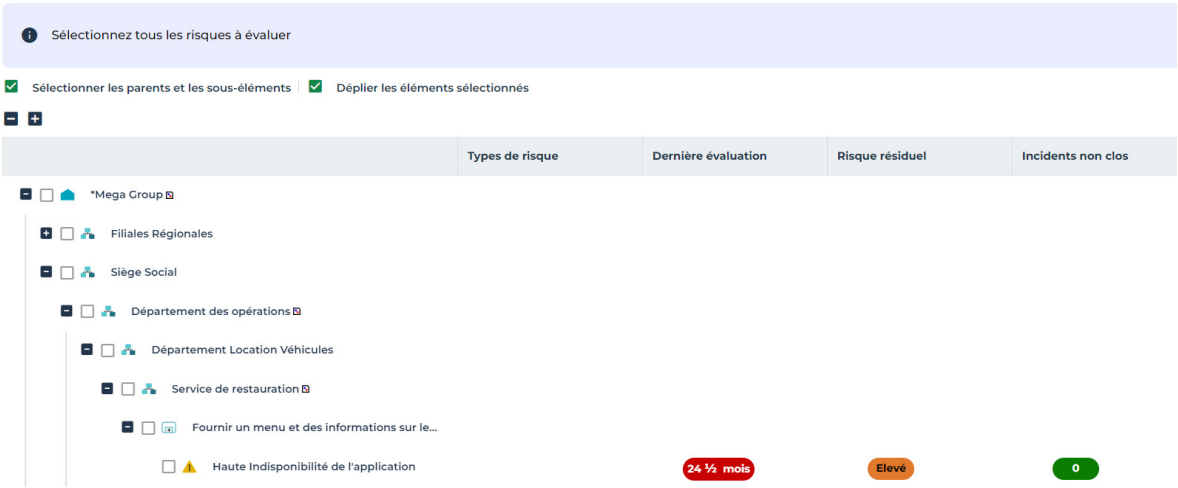
     ☛ *Pour plus de détails, voir Modèles d'évaluation pour les risques.*
   - **Évaluation des contrôles**
   - **Évaluation des contrôles par entité et texte de référence**

     ☛ *Pour plus de détails, voir Modèles d'évaluation pour les contrôles.*
4. Cliquez sur **Suivant**.
   La page de création d'une campagne apparaît.
5. Indiquez le **Nom** de la campagne.
6. Modifiez éventuellement le **Calendrier**.

   ☛ *Le calendrier sert à initialiser les dates de début et de fin de la campagne d'évaluation.*
7. Indiquez la **Date de Début** et la **Date de fin**.
8. Cliquez sur **Suivant**.

9. Dans la fenêtre **Sélection du périmètre**, sélectionnez les objets qui définissent le contexte de l'évaluation.
   L'arborescence vous permet de sélectionner les contrôles ou les risques évalués ***dans leur contexte***.
   Un contrôle ou un risque est évalué dans le contexte des éléments de la branche qui remonte de l'objet en question jusqu'à la racine.

   ☛ *Des colonnes vous donnent des indications pour vous permettre de décider quels risques ou contrôles méritent d'être évalués.*

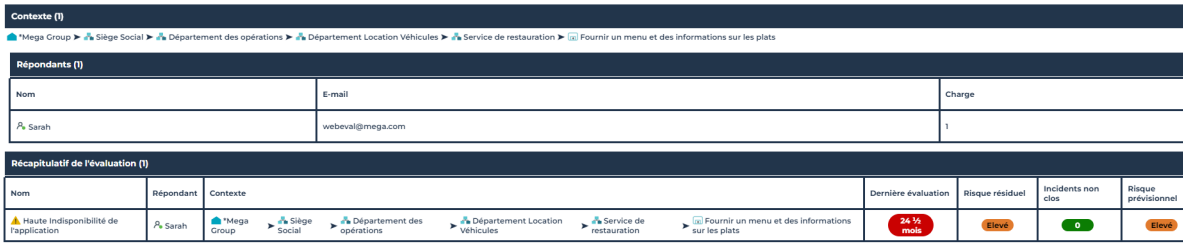


Dans l'exemple ci-dessus, si vous avez sélectionné l'entité "Département des opérations", tous les risques et objets contextes se situant à un niveau inférieur sont sélectionnés, ainsi que tous les objets contextes parents jusqu'à la racine de l'arborescence.

☛ *Si vous dé-sélectionnez un nœud d'une branche, seuls les enfants de cette branche sont dé-sélectionnés.*

10. Cliquez sur **Suivant**.

11. Étudiez le récapitulatif de votre campagne.
Les éléments qui vont être évalués apparaissent.



Vous pouvez visualiser notamment :

- les ***caractéristiques évaluées*** (définies dans le modèle d'évaluation)
- les ***objets*** (risques ou contrôles) évalués
- les ***objets contextes*** (entités, processus, etc.)
- les ***nœuds d'évaluation***, qui correspondent aux objets placés dans les différents objets contextes, associés aux répondants.
- les ***répondants***
- les ***erreurs*** éventuelles (sans certaines informations, par exemple les répondants, la campagne ne peut pas être lancée)
- des ***avertissements***, à titre informatif (par exemple : l'e-mail des répondants manque)

12. Cliquez sur **Suivant**.
13. Dans la page de planification, spécifiez à quel moment vous voulez lancer la campagne :
    - **Immédiatement**

      ☛ *Si vous choisissez cette option, le lancement de la campagne est effectuée sous vos yeux (dès que vous cliquez sur **OK**).*
    - **Date et heure spécifiques**

      ☛ *Vos questionnaires seront envoyés aux répondants à la date et à l'heure spécifiées. Il s'agit de l'option recommandée.*
    - **Pas maintenant**

      ☛ *Aucun questionnaire ne sera envoyé. Vous devrez créer manuellement une session d'évaluation une fois que vous serez prêt à planifier vos questionnaires dans le temps. Voir Créer manuellement une session d'évaluation.*

      ☛ *Cette option n'est pas disponible si vous avez choisi de créer la campagne d'évaluation sans modèle.*
14. Cliquez sur **OK**.

Créer manuellement une session d'évaluation

Vous devez créer manuellement une (ou plusieurs) session(s) d'évaluation si vous avez sélectionné l'option de planification "Pas maintenant" lors de la création de votre campagne d'évaluation.

☛ *Voir Etape précédente : Créer une campagne d'évaluation.*

Pour créer une session d'évaluation :

1. Dans la fenêtre de propriétés de la campagne d'évaluation, sélectionnez la page **Sessions**.
2. Cliquez sur **Nouveau** et cliquez sur **Suivant**.
3. Sélectionnez le périmètre de la session, c'est-dire les objets à évaluer dans leur contexte.

☛ *Seuls les objets valides (pour lesquels un répondant existe et un e-mail a été renseigné) peuvent être sélectionnés.*

4. Cliquez sur **Suivant**.
5. Dans la fenêtre de planification, choisissez si vous voulez envoyer les questionnaires :
   - **Immédiatement**

     ☛ *Si vous avez choisi "Immédiatement", une session se lance automatiquement.*

   - à une **Date et Heure spécifiques**

RAPPORTS DES SOLUTIONS GRC

Des rapports communs aux diverses problématiques GRC (Government, Risk & Compliance) vous sont proposés.

- Rapports d'indicateurs clés
- Rapports de suivi des plans d'action

Pour le détail des rapports spécifiques à chaque solution, voir la documentation correspondante :

- Rapports concernant les risques
- Rapports concernant les contrôles
- Rapports de conformité informatique et réglementaire
- Rapports concernant les incidents

Un tableau de synthèse donne des indications sur la disponibilité des rapports. Voir Disponibilité des rapports GRC.

☛ *Pour plus de détails sur les rapports, voir :*

- *Accéder aux rapports*
- *Créer un rapport*
- *Gérer les propriétés d'un rapport*

DISPONIBILITÉ DES RAPPORTS GRC

Les rapports disponibles varient selon le profil avec lequel vous êtes connecté et la solution dont vous disposez.

Profils/Thématiques	Risques	Contrôles	Conformité	Inci-dents	Plans d'action
Manager GRC	X	X	X	X	X
Risk Manager	X				X
Directeur du contrôle interne		X	X		X
Gestionnaire des inci-dents et des pertes	X		X	X	X

Voir aussi :

- Rapports de suivi des plans d'action
- Rapports de conformité informatique et réglementaire

RAPPORTS D'INDICATEURS CLÉS

☛ *Pour plus de détails sur les indicateurs clés, voir Indicateurs clés.*

Hopex GRC propose plusieurs rapports pour comparer les indicateurs clés.

Les rapports suivants sont disponibles :

- Comparateur d'indicateurs
- Jauges multi-indicateurs
- Graphe multi-indicateurs

☛ ***Hopex GRC** permet d'afficher un graphique spécifique à un indicateur clé. Pour plus de détails, voir Visualiser le graphique d'indicateur.*

Comparateur d'indicateurs

Ce rapport vous permet de comparer deux indicateurs clés sur un même graphique à ligne.

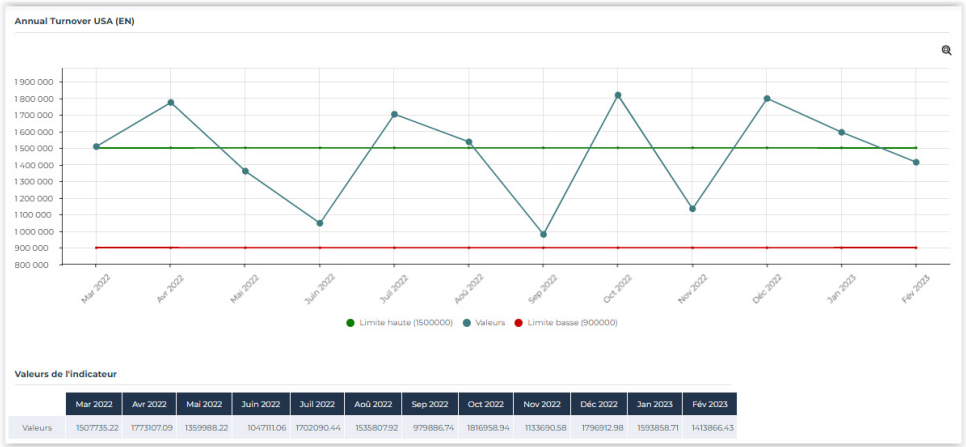
Chemin d'accès

Barre de navigation > Rapports

Paramètres

Parameters	Remarques
Indicateur clé 1	Obligatoire
Indicateur clé 2	Obligatoire
Période d'agrégation	Obligatoire
Méthode d'agrégation	Obligatoire
Date de début des valeurs	Optionnel
Date de fin des valeurs	Optionnel

Résultats



Jauges multi-indicateurs

Ce rapport permet d'afficher plusieurs indicateurs au moyen de jauges.

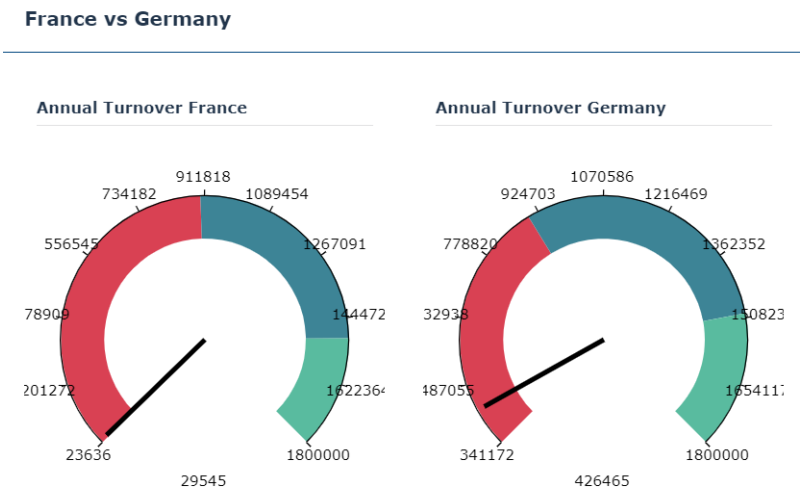
Chemin d'accès

Barre de navigation > Rapports

Paramètres

Paramètres	Remarques
Nombre de colonnes	Obligatoire - Vous pouvez choisir le nombre de colonnes qui convient le mieux pour afficher vos indicateurs.
Indicateurs clés	Obligatoire
Date de début des valeurs	Obligatoire
Date de fin des valeurs	Obligatoire

Résultats



Graphe multi-indicateurs

Ce rapport permet d'afficher plusieurs indicateurs dans des graphiques multi-lignes.

Chemin d'accès

Barre de navigation > Rapports

Paramètres

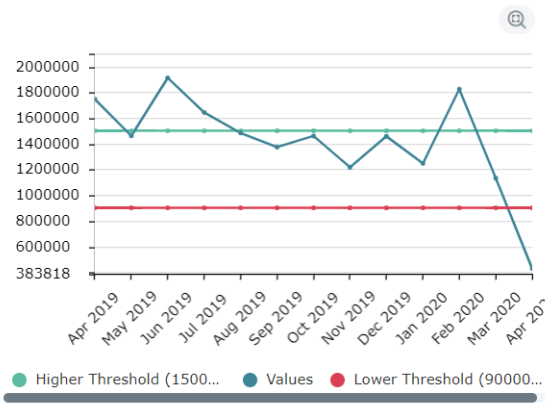
Paramètres	Remarques
Nombre de colonnes	Obligatoire
Indicateurs clés	Obligatoire
Date de début des valeurs	Optionnel
Date de fin des valeurs	Optionnel

Résultats

France vs. Germany

Annual Turnover France

Annual Turnover Germany



RAPPORTS DE SUIVI DES PLANS D'ACTION

Plus de détails sur les plans d'action, voir Utiliser les plans d'action.

Pour accéder à ces rapports :

- Dans la barre de navigation, sélectionnez **Rapports**.

Suivi des plans d'action (tableau de bord)

Paramètres

Paramètres	Contrainte
Plans d'actions ou Bibliothèques	Obligatoire

Résultat

Priorité des plans d'action

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur priorité.

Les priorités possibles sont les suivantes :

- Critique
- Élevée
- Moyenne
- Basse

Plans d'action par niveau organisationnel

- global
- local

Plans d'action par statut

- À soumettre
- À valider
- À envoyer
- En cours
- Terminé
- Rejeté

Plans d'action par origine

- Audit
- Conformité
- Événement
- Autre
- RFC
- Risque

Plans d'action par catégorie

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur catégorie.

Quelques exemples de catégories de plans d'action possibles :

- Réduction des impacts
- Amélioration de la pertinence des contrôles
- ...

Réalisation des plans d'action

- Succès
- Échec
- Non évalué

Top 10 des plans d'action

Liste des 10 plans d'action ayant la priorité la plus haute

Rapport de suivi des plans d'action (tableau de bord)

Paramètres

Paramètres	Contrainte
Date de début	
Date de fin	
Entités	Facultatif
Processus	Facultatif

Résultat

Le nombre de plans d'action est affiché.

Plusieurs graphes présentent la répartition des plans d'action en fonction de différents critères.

Plans d'action par statut

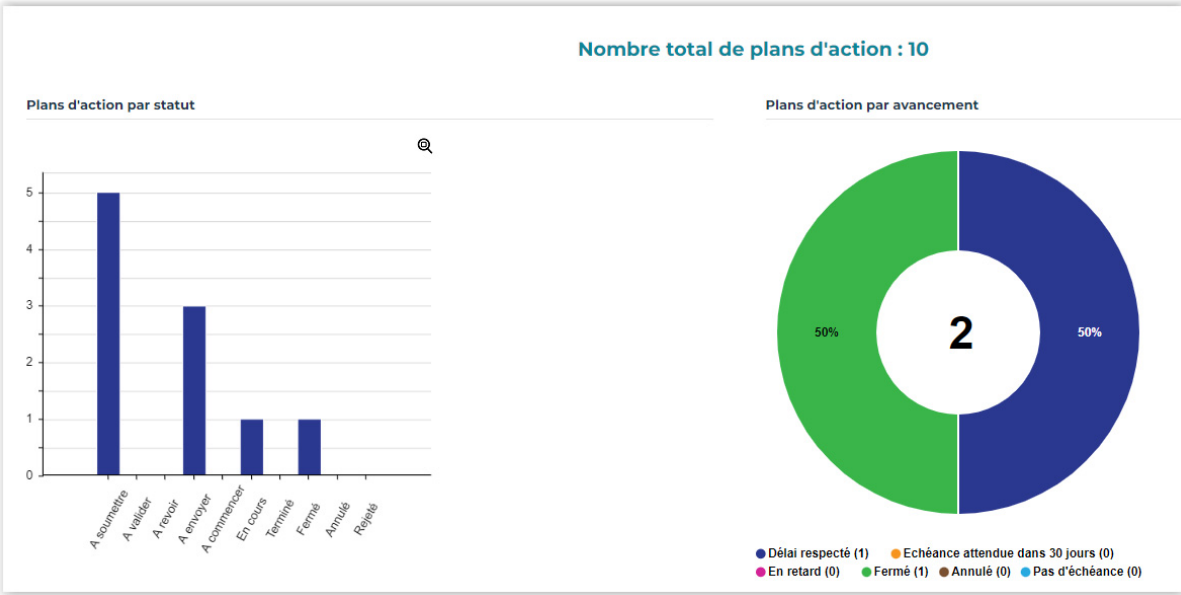
Ce diagramme en barres présente les statuts des plans d'action :

- À soumettre
- À valider
- À revoir
- À envoyer
- À commencer
- En cours
- Terminé
- Fermé
- Annulé

Plans d'action par avancement

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur statut. Les statuts possibles sont les suivants :

- Dans les temps :
  - en cours
  - avec une date d'échéance supérieure à 30 jours
- En retard :
  - en cours
  - avec une date d'échéance antérieure à la date courante
- Arrivant à échéance :
  - en cours
  - avec une date d'échéance comprise entre 0 et 30 jours
- Annulé
- Fermé



Plans d'action par priorité

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur priorité.

Les priorités possibles sont les suivantes :

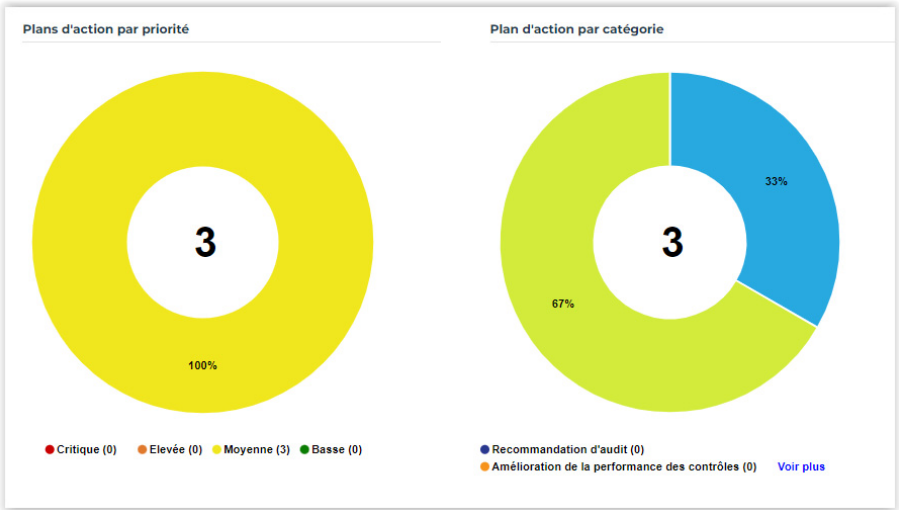
- Critique
- Élevée
- Moyenne
- Basse

Plans d'action par catégorie

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur catégorie.

Quelques exemples de catégories de plans d'action possibles :

- Recommandation d'audit
- Réduction des impacts
- Amélioration de la pertinence des contrôles
- ...



Plan d'action par nature

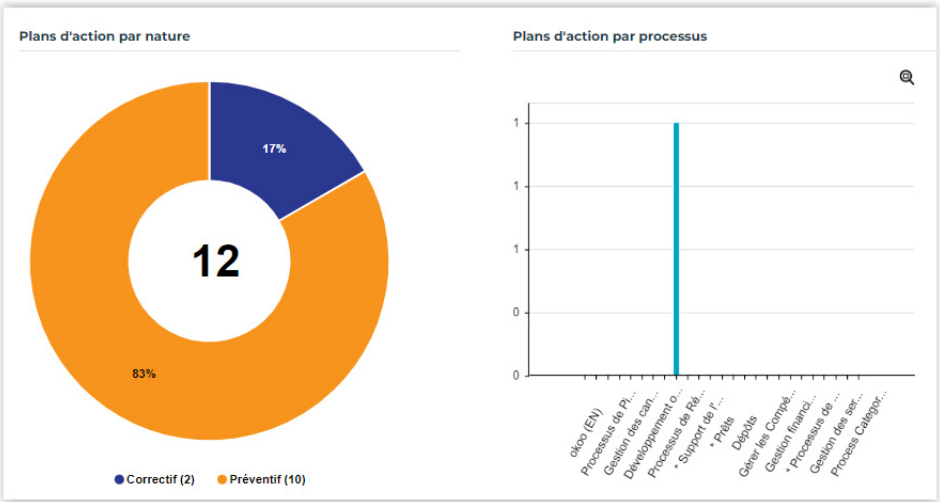
- préventif
- correctif

Plans d'action par processus

Ce diagramme en barres présente le découpage des plans d'action pour chaque processus.

- En abscisse : tous les processus (métiers et organisationnels)
- en ordonnée : nombre de plans d'action liés à chacun des processus et ses sous-processus

> ☛ *Si aucun processus n'est sélectionné, tous les processus racines sont pris par défaut.*

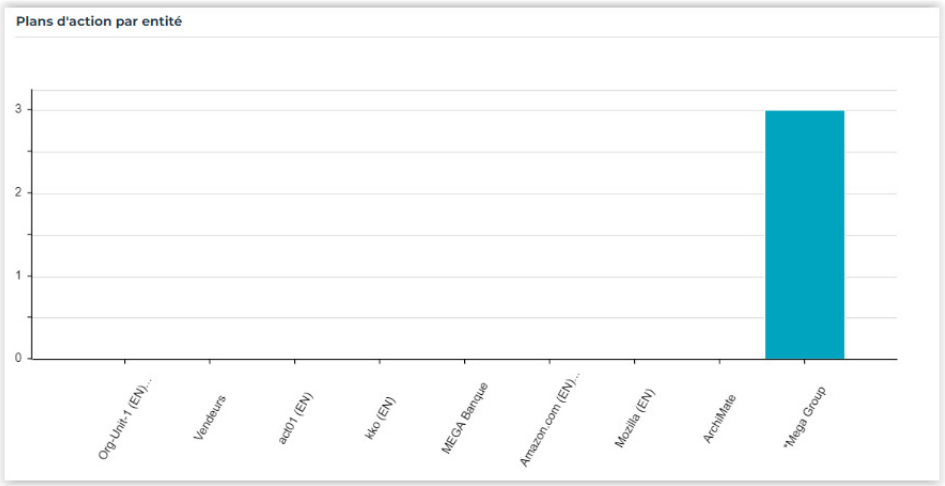


Plans d'action par entité

Ce diagramme en barres présente le découpage des plans d'action pour chaque entité.

- En abscisse : toutes les entités
- en ordonnée : nombre de plans d'action liés à chacune des entités et sous-entités

> ☛ *Si aucune entité n'est sélectionnée, toutes les entités racines sont prises par défaut.*



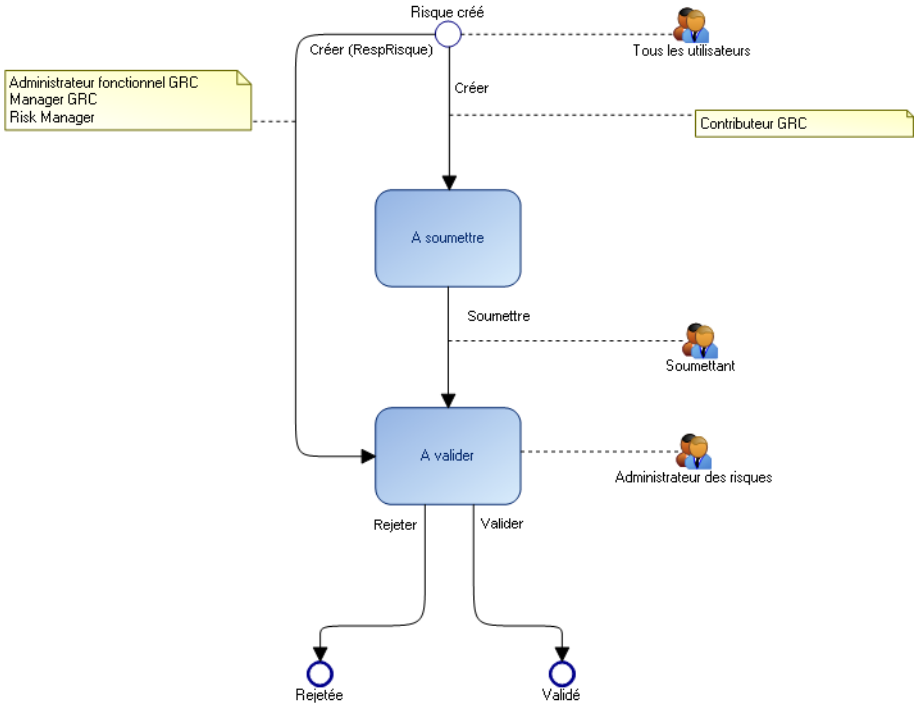
WORKFLOWS DES SOLUTIONS GRC

Le déroulement des activités GRC (Governance, Risk & Compliance) s'effectue via des workflows.

Les transitions de workflow sont disponibles dans le menu contextuel des objets sur lequel le workflow porte.

- ✓ Workflows liés aux risques
- ✓ Workflows liés au testing
- ✓ Workflows liés aux plans d'action
- ✓ Workflow des incidents
- ✓ Workflow des campagnes

WORKFLOWS LIÉS AUX RISQUES

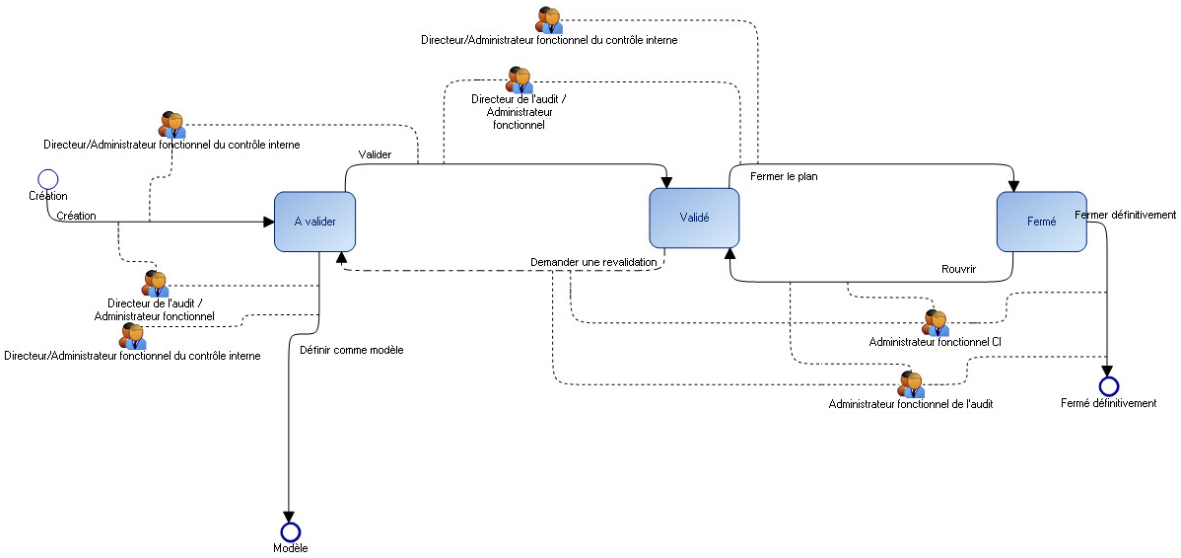


☛ *Pour plus de détails sur les risques et le workflow des risques, voir Gérer les risques.*

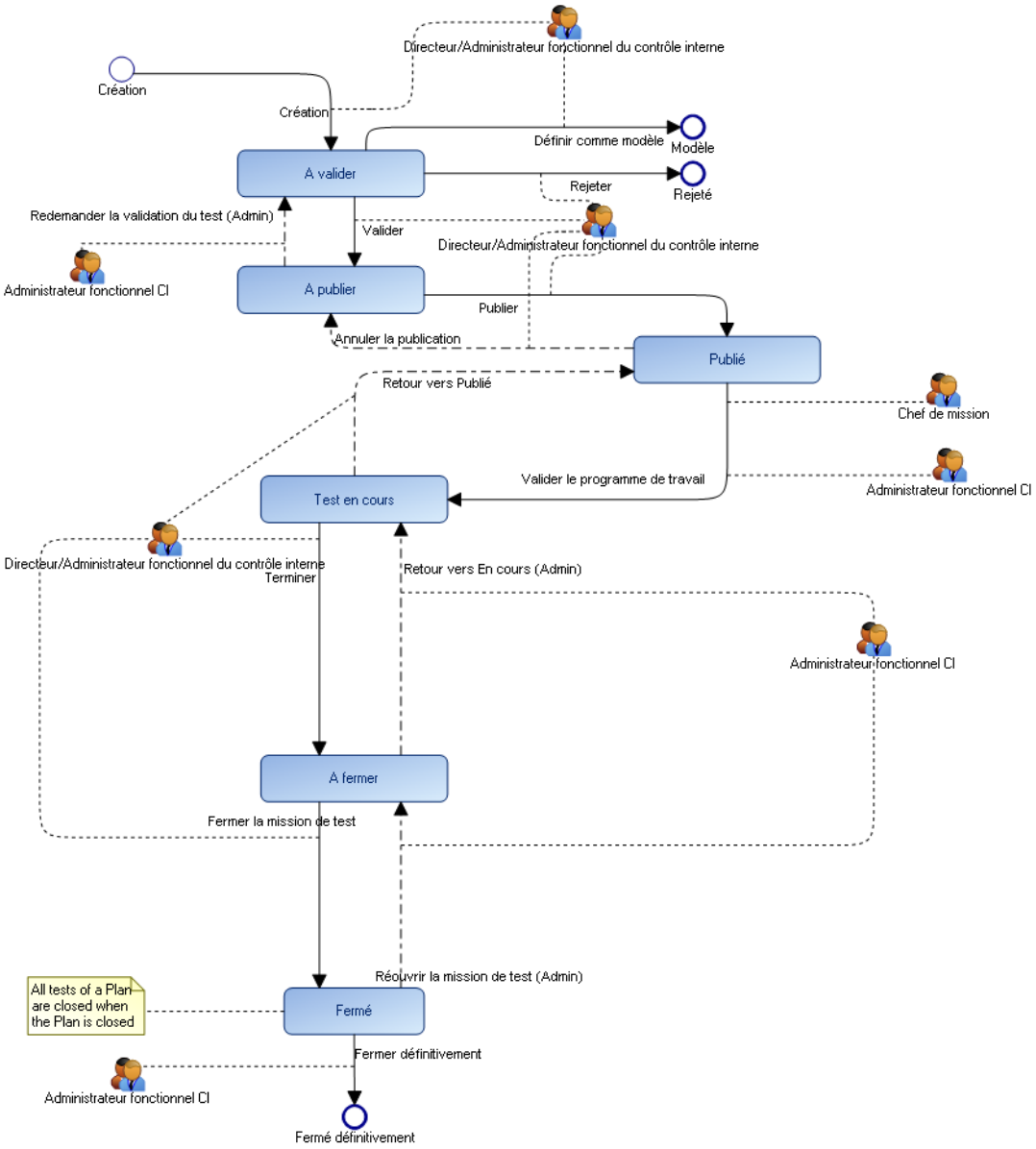
WORKFLOWS LIÉS AU TESTING

☛ *Pour plus de détails sur le testing, voir Tester les contrôles.*

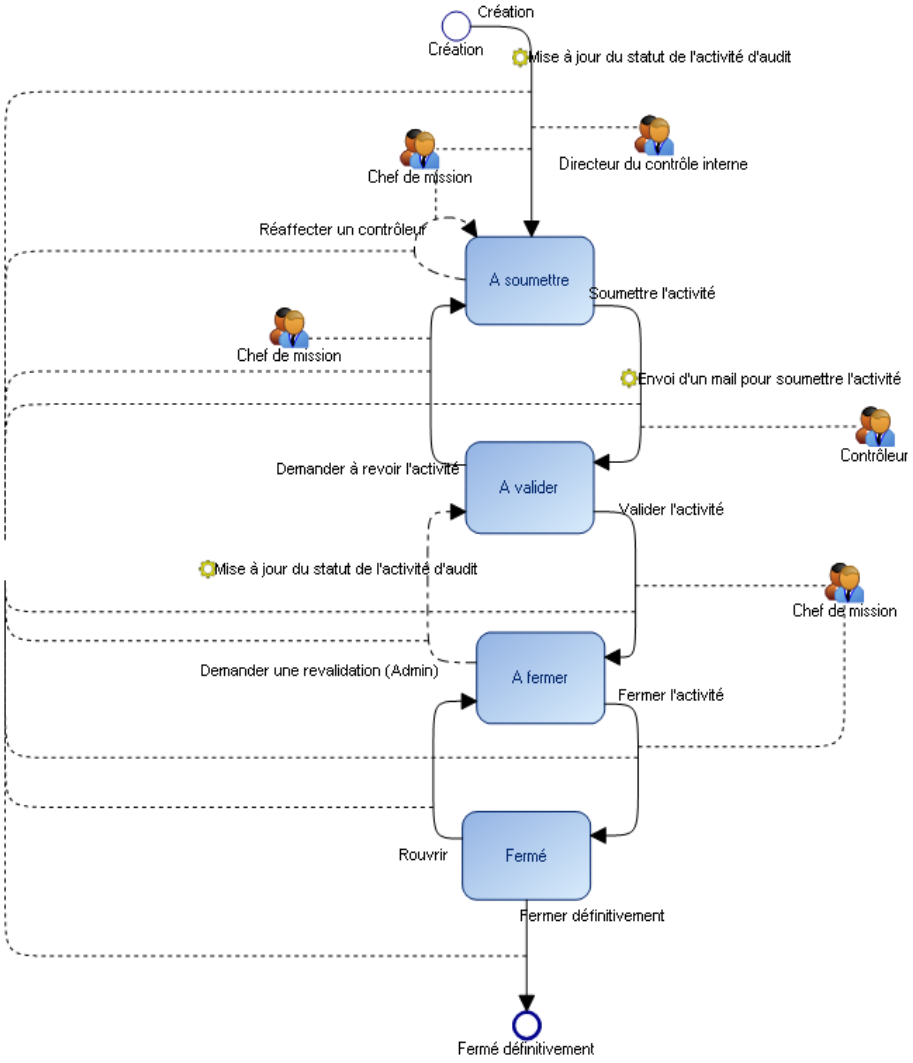
Workflow des plans de test / d'audit



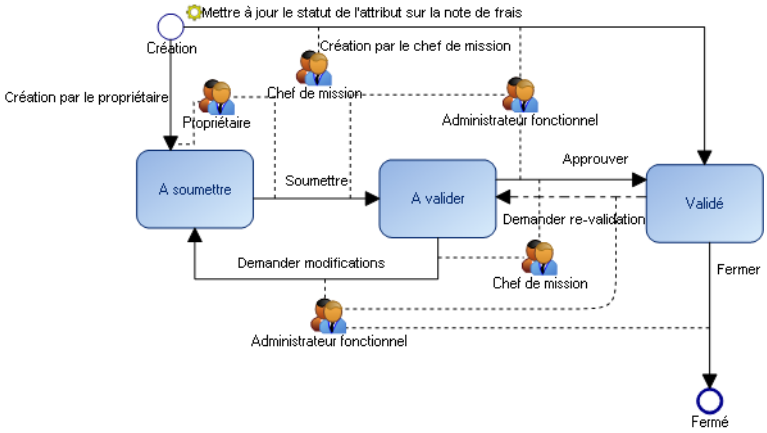
Workflow des missions de test



Workflow des activités de test



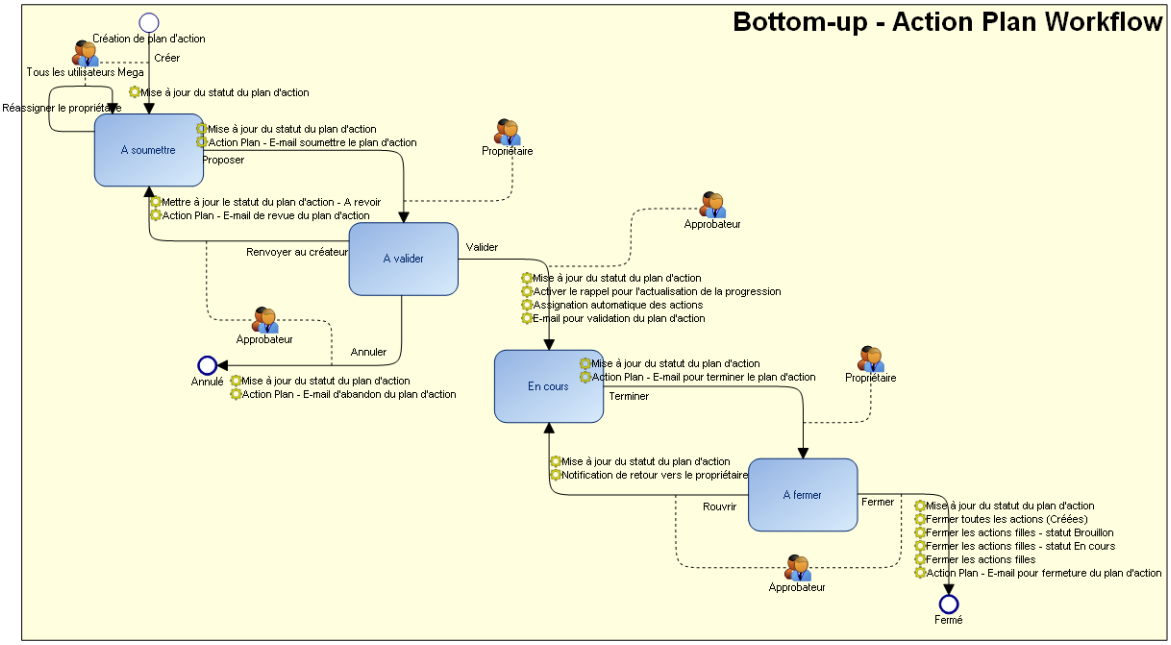
Workflow des notes de frais



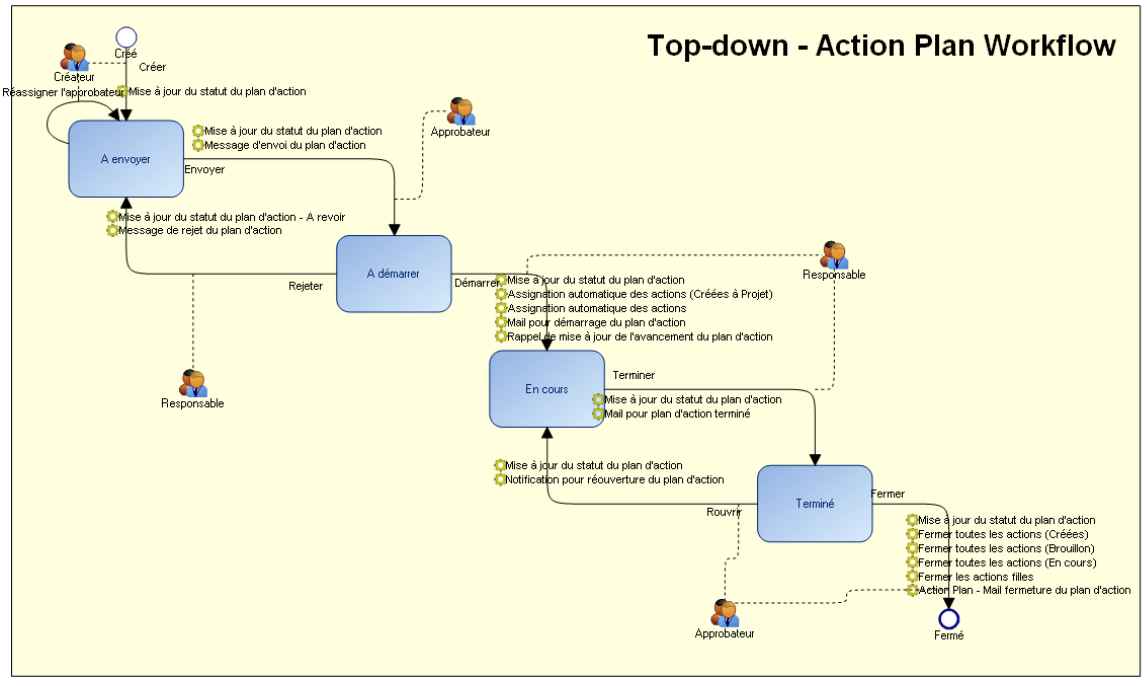
WORKFLOWS LIÉS AUX PLANS D'ACTION

☛ *Pour plus de détails sur les plans d'action, voir Utiliser les plans d'action.*

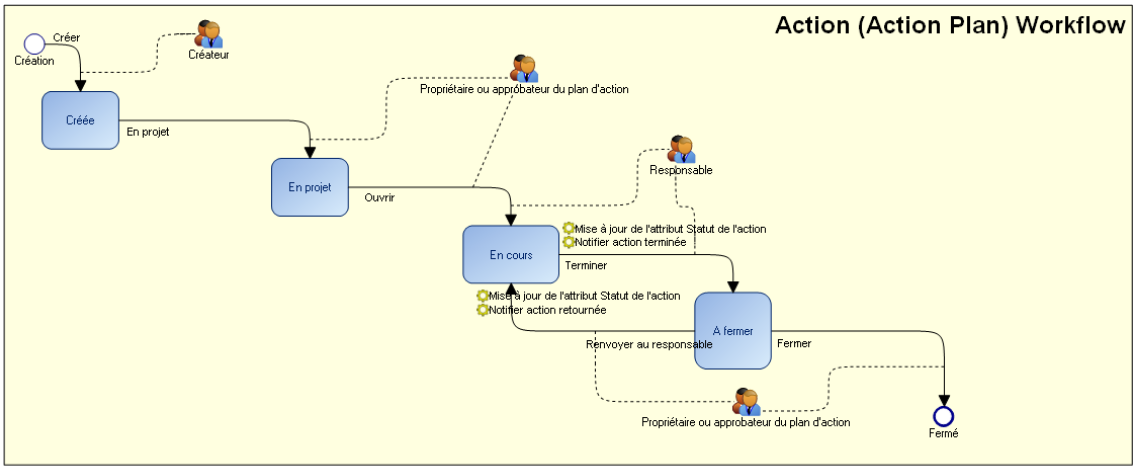
Workflow de plan d'action "bottom-up"

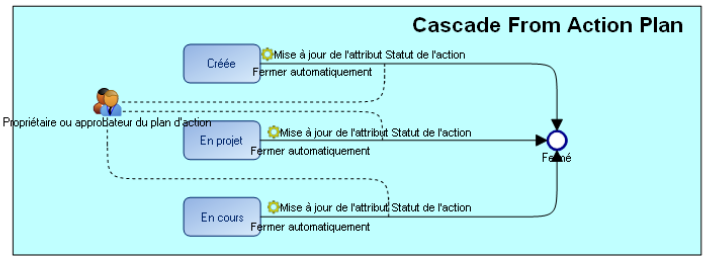


Workflow de plan d’action "top-down"

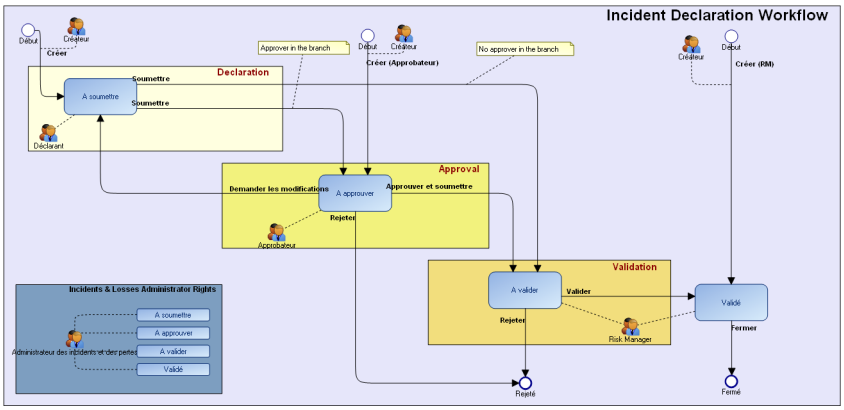


Workflow d'actions





WORKFLOW DES INCIDENTS



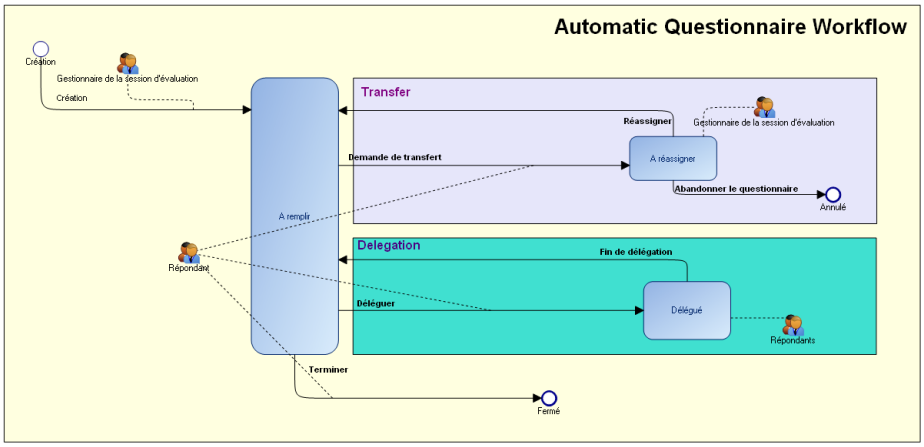
☛ *Pour plus de détails sur les incidents, voir Le processus de gestion d'un incident.*

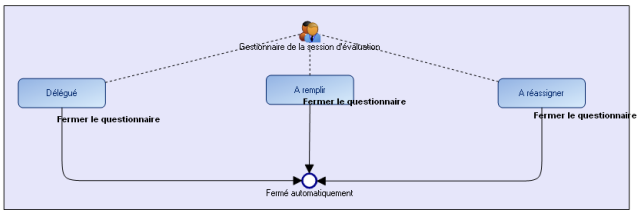
WORKFLOW DES CAMPAGNES

Workflow des campagnes d'évaluation

Voir Workflows génériques des évaluations.

Workflow des campagnes d'exécution (automatiques)





BUREAU DES CONTRIBUTEURS GRC

Un bureau spécifique permet de contribuer aux problématiques GRC (Governance, Risk & Compliance).

Ce bureau est disponible pour les utilisateurs métier des solutions suivantes :

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

☛ *Vous avez accès aux menus et fonctionnalités qui concernent la (ou les) solution(s) dont vous disposez.*

✓ Présentation du bureau des Contributeurs GRC
✓ Consulter votre environnement
✓ Tableau de bord et widgets
✓ Gérer les incidents
✓ Gérer les plans d'action et actions
✓ Gérer les recommandations
✓ Gérer les questionnaires et check-lists
✓ Créer des risques et contrôles
✓ Gérer les indicateurs clés
✓ Réaliser un BIA (Bilan d'Impact sur l'Activité)
✓ Participer aux Plans de Continuité de l'Activité

Présentation du bureau des Contributeurs GRC

Accéder au bureau des contributeurs GRC

Pour accéder au bureau des contributeurs GRC :

1. Voir Se connecter à Hopex.
2. Connectez-vous avec le profil "Contributeur GRC".

Fonctionnalités disponibles pour le contributeur GRC

Ci-dessous les types d'objets et fonctionnalités disponibles selon les solutions.

Fonctionnalités/Solutions	ERM	IC	LDC	Audit	BCM
Généralités - Visualiser l'environnement (Consulter votre environnement) - Visualiser et exporter les rapports du tableau de bord	X	X	X	X	
Risques - Identifier les risques - Répondre aux questionnaires d'évaluation (Voir : Répondre à un questionnaire)	X				
Contrôles - Créer des contrôles - Répondre aux questionnaires d'évaluation (Voir : Répondre à un questionnaire)	X	X			
Exécution des contrôles - Compléter les check-lists d'exécution (Voir Remplir des check-lists d'évaluation)		X			
Plans d'action/Actions - Visualiser et modifier les plans d'action - Créer des actions (Voir Gérer les plans d'action et actions)	X	X	X	X	
Recommandations - Visualiser les recommandations (Voir Gérer les recommandations)				X	
Incidents - Déclarer des incidents (Voir Gérer les incidents)			X		
Indicateurs clés - Saisir une valeur d'indicateur clé (Voir Saisir une valeur d'indicateur clé)	X	X			
Bilan d'Impact sur l'Activité - Remplir une matrice d'analyse de BIA (Voir Réaliser un BIA (Bilan d'Impact sur l'Activité))					X
Participer aux Plans de Continuité d'Activité (PCA) : - testés dans le cadre d'exercices - déclenchés dans le cadre de crises (voir Participer aux Plans de Continuité de l'Activité)					X

Page d'accueil

La page d'accueil permettent de réaliser les tâches les plus courantes sur les objets sur lesquels vous devez intervenir.

☛ *Les menus affichés dépendent de la (des) solution(s) dont vous disposez.*

Vous pouvez par exemple créer un incident, répondre à des questionnaires, renseigner le pourcentage d'avancement de vos plans d'action.

Tableau de bord

Vous pouvez y ajouter des widgets adaptés aux diverses problématiques GRC.

Voir :

- Personnaliser votre tableau de bord
- Tableau de bord et widgets

Mes tâches

Vous pouvez accéder aux objets qui vous concernent - directement ou indirectement - et sur lesquels vous devez/pouvez intervenir.

Voir :

- Gérer les questionnaires et check-lists
- Créer des risques et contrôles
- Gérer les indicateurs clés
- Réaliser un BIA (Bilan d'Impact sur l'Activité)
- Participer aux Plans de Continuité de l'Activité
- Gérer les plans d'action et actions
- Gérer les recommandations

Environnement

Dans cette section vous retrouvez les objets susceptibles de constituer le périmètre des objets sur lesquels vous intervenez.

- Entités
- Processus
- Applications
- Lignes métier

Pour plus de détails, voir Consulter votre environnement.

Risques

🕮 *Un risque est un danger plus ou moins probable auquel est exposée une organisation.*

Ce menu permet d'accéder :

- à vos risques : risques dont vous êtes propriétaire
- aux risques de votre périmètre : risques pour lesquels vous êtes correspondant/évaluateur dans le cadre d'au moins un objet de votre périmètre.

Pour plus de détails sur les caractéristiques des risques, voir Caractéristiques d'un risque.

Contrôles

Ce menu liste tous les contrôles dont vous êtes responsable (pour au moins une des entités du périmètre).

> 🕮 *Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.*

Pour plus de détails, voir Caractéristiques d'un contrôle.

Incidents

Ce menu liste les incidents :

- que vous avez déclarés
- de votre périmètre : incidents concernant au moins l'un des objets de votre périmètre

> 🕮 *Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.*

Pour plus de détails, voir Gérer les incidents.

CONSULTER VOTRE ENVIRONNEMENT

Pour accéder aux objets de votre environnement :

- Cliquez sur **Environnement** puis sélectionnez le sous-menu qui vous intéresse.

☛ *Pour la description détaillée de ces objets, voir Environnement GRC.*

Processus

📖 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

📖 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

Pour plus de détails, voir Gérer les catégories de processus et processus.

Applications

📖 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

Pour plus de détails, voir Gérer les applications.

Lignes métier

📖 *Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.*

Pour plus de détails, voir Gérer les lignes métier.

Entités

📖 *L'évaluation est un mécanisme qui permet de lancer des questionnaires à une population identifiée afin d'obtenir des estimations (qualitatives ou quantitatives) sur des objets identifiés.*

Pour plus de détails, voir Gérer les entités.

TABLEAU DE BORD ET WIDGETS

Votre tableau de bord permet d'ajouter des widgets généraux ou spécifiques à la GRC.

Pour ajouter des widgets à votre tableau de bord :

1. Cliquez sur **Tableau de bord**.
2. Cliquez sur le signe + pour ajouter un widget à votre bureau.
3. Sélectionnez un widget dans la liste.
   Celui-ci apparait sur votre bureau.

Widgets concernant les plans d'action

☛ *Les widgets concernant les plans d'action sont disponibles dans toutes les solutions GRC.*

Plans d'action par avancement

Ce diagramme circulaire présente la répartition des plans d'action selon leur statut d'avancement :

- En retard
- Dans les temps
- Pas de date d'échéance
- Échéance d'ici 30 jours
- Annulé
- Fermé
- En retard

Plans d'action par priorité

Ce diagramme circulaire affiche la répartition des plans d'action par priorité :

- Critique
- Elevée
- Moyenne
- Basse

Plans d'action par statut

Ce graphique à barres présente la répartition des plans d'action dont vous êtes responsable (par statut) :

- A démarrer
- En cours
- Terminé

Tableau de bord des plans d'action

Ce diagramme circulaire présente les actions "en retard" ou "dans les temps" dont vous êtes responsable.

Widget spécifique à la GRC

Risques par statut : ce diagramme circulaire affiche la répartition par statut des risques détenus par le contributeur GRC.

Widgets spécifiques à Hopex Internal Audit

Voir Consulter les widgets concernant les recommandations.

GÉRER LES INCIDENTS

Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.

> ☛ *Les incidents sont disponibles avec **Hopex LDC**. Pour plus de détails, voir Collecte des incidents.*

Le profil "Contributeur GRC" permet de :

- Créer un incident, le modifier avant de le soumettre, le supprimer
- Analyser un incident (contexte et pertes)
- Approuver un incident qui vient d'être déclaré
- Définir et mettre en œuvre des plans d'action

> ☛ *Pour plus de détails, voir Gérer les plans d'action et actions.*

Créer un incident

Pour créer un incident :

1. Voir Accéder au bureau des contributeurs GRC.
2. Dans la page d'accueil, partie **Accès rapide**, cliquez sur **Créer un incident**.
3. Sélectionnez l'**Entité du déclarant**.
4. Cliquez sur **Relier** puis sur **OK**.

Pour plus de détails sur les incidents, voir la documentation correspondante de la solution **Hopex LDC** : Collecte des incidents.

Accéder aux incidents

Pour accéder à vos incidents:

- Depuis le bureau, cliquez **Incidents.**
  Les incidents que vous avez créés apparaissent.

GÉRER LES PLANS D'ACTION ET ACTIONS

Un plan d'action est constitué d'une série d'actions, avec pour objectif de réduire les risques et les événements ayant un impact négatif sur l'activité de l'entreprise.

> ☛ *Les plans d'actions sont utilisés dans le cadre de toutes les solutions GRC, sauf dans **Hopex Internal Audit** (où les recommandations et actions sont utilisées).*

Contexte de création d'un plan d'action

Deux types de workflow sont disponibles pour les plans d'action :

- top-down
- bottom-up

Les actions que vous pouvez effectuer à partir du bureau du contributeur dépendent de la solution que vous utilisez et du workflow mis en place dans votre entreprise.

Vous pouvez, en tant que contributeur, être amené à créer un plan d'action dans différents contextes, par exemple :

- Dans une approche "bottom-up" : vous pouvez créer un plan d'action lorsque vous répondez aux questionnaires des exigences.

  > ☛ *Vous devez dans ce cas le soumettre via le workflow pour qu'un approbateur puisse le valider.*

- Un auditeur peut constater une défaillance et vous demander de créer un plan d'action pour la traiter.

  > ☛ *Vous devez dans ce cas relier la défaillance au plan d'action.*

Accéder aux plans d'action

Pour accéder aux plans d'action :

❱ Dans la barre de navigation, sélectionnez **Mes tâches > Plans d'action**.

Relier une défaillance à un plan d'action

Pour relier une défaillance à un plan d'action :

1. Dans la fenêtre de propriétés du plan d'action, dépliez la section **Périmètre** et sélectionnez l'onglet **Défaillances**.
2. Cliquez sur **Relier**.

   > ☛ *Vous pouvez également créer une défaillance si nécessaire.*

Renseigner l'avancement d'un plan d'action

Vous devez rendre compte de l'avancement de votre plan d'action. Pour cela, vous pouvez créer des états de manière régulière.

Pour renseigner l'avancement :

1. Ouvrez la fenêtre de propriétés du plan d'action.

2. Dépliez la section **Avancement du plan d'action** et dans le cadre **Etat d'avancement** cliquez sur **Nouveau**.
3. Spécifiez un **Pourcentage d'avancement**.
4. Donnez une **Evaluation** de l'avancement.
   Vous pouvez préciser si le plan d'action est :
   - dans les temps
   - en retard

Gérer les actions

Dans le cadre de l'audit interne ou des activités de testing, vous pouvez, en tant que responsable ou correspondant d'action, être amené à :

- spécifier les actions à entreprendre pour assurer les suivi des recommandations

  ☛ *Voir Mettre en oeuvre les recommandations.*
- vous assurer de la bonne implémentation des actions

Pour accéder à vos actions :

1. Voir Accéder au bureau des contributeurs GRC.
2. Dans la barre de navigation, sélectionnez **Mes tâches > Plans d'action > Actions**.

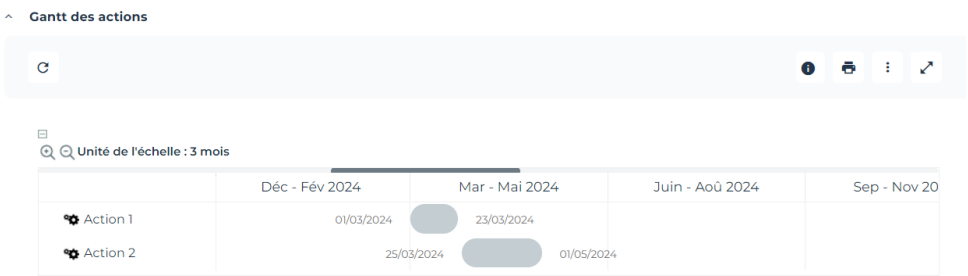
Voir aussi Créer une action dans le cadre d'une recommandation.

Visualiser le Gantt des actions

Hopex vous permet de visualiser le planning des actions sous forme de diagramme de Gantt.

Pour accéder au diagramme de Gantt des actions :

1. Dans la barre de navigation, sélectionnez **Mes tâches > Plans d'action**.
2. Ouvrez les propriétés d'un plan d'action et sélectionnez la page **Actions**.
   Dans la partie inférieure de la page, le Gantt des actions apparaît :



GÉRER LES RECOMMANDATIONS

☛ *Les recommandations sont utilisées dans le cadre de **Hopex Internal Audit**.*

🕮 *Une recommandation décrit ce qui doit être réalisé pour corriger une non-conformité détectée durant l'audit.*

Accéder aux recommandations

Pour accéder à vos recommandations :

1. Dans la barre de navigation, sélectionnez **Mes tâches > Recommandations**.

Dans la page qui s'affiche, les recommandations sont classées en fonction de leur statut :

- Recommandations
- Recommandations en retard

Mettre en oeuvre les recommandations

Vous pouvez être amené à gérer des recommandations qui découlent des activités de testing ou de l'envoi du rapport d'audit final.

En tant que responsable de recommandation, vous pouvez :

- créer des actions ayant pour objectif de mettre en œuvre les recommandations.
- indiquer un pourcentage d'avancement sur vos actions

Pour plus de détails sur les recommandations dans le cadre de **Hopex Internal Audit** : Mettre en œuvre les recommandations

Créer une action dans le cadre d'une recommandation

Pour créer une action :

1. Voir Accéder aux recommandations
2. Dans les propriétés de la recommandation, sélectionnez la page **Plan d'action**.
3. Dans la section **Actions**, cliquez sur **Nouveau**.
4. Ouvrez les propriétés de l'action créée.
5. Modifiez éventuellement son nom, saisissez une date limite ainsi qu'un **Propriétaire**.

   ☛ *La liste disponible dans le champ **Propriétaire** correspond à la liste des audités définie sur la mission d'audit.*

Soumettre un plan d'action (de recommandations)

Les actions créées et affectées aux utilisateurs appropriés dans le cadre de **Hopex Internal Audit** constituent un plan d'action.

Vous pouvez le soumettre au chef de mission ou au directeur d'audit via le workflow de recommandations.

Pour cela :

1. Voir Accéder aux recommandations
2. Cliquez sur le nom de la recommandation et sélectionnez **Plan d'action à soumettre** > **Soumettre le plan d'action**.

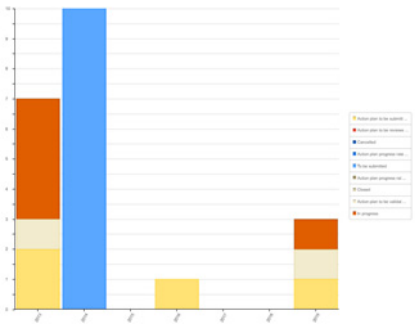
   ☛ *Le chef de mission ou le directeur d'audit valide le plan d'action en retour.*

Consulter les widgets concernant les recommandations

Recommandations par statut et année

Ce graphique à barres affiche les recommandations :

- par année
- par statut (chaque couleur correspondant à un statut différent)



Recommandations par statut et mission d'audit

Ce graphique à barres affiche les recommandations :

- par mission d'audit
- par statut (chaque couleur correspondant à un statut différent)

Tableau de bord des recommandations

Ce tableau de bord affiche la répartition des actions par avancement pour toutes les recommandations en cours dont vous êtes responsable :

- En retard
- Dans les temps

GÉRER LES QUESTIONNAIRES ET CHECK-LISTS

Un questionnaire d'évaluation est une liste de questions portant sur un objet particulier et adressée à des utilisateurs.

Vous pouvez être amené à répondre à des questionnaires concernant les contrôles dans le cadre du contrôle interne.

📖 *Une check-list est un cas particulier de questionnaire utilisé dans le cadre de **Hopex Internal Control** pour l'exécution des contrôles.*

Accéder aux questionnaires

Pour accéder aux questionnaires :

1. Voir Accéder au bureau des contributeurs GRC.
2. Dans la page d'accueil, cliquez sur **Mes tâches > Questionnaires**.

Dans la page qui s'affiche, les questionnaires sont classés comme suit :

- Questionnaires
- Questionnaires en retard

Répondre à un questionnaire

Pour remplir un questionnaire :

1. Voir Accéder aux questionnaires.
2. Cliquez sur le questionnaire qui vous intéresse.
3. Sélectionnez tour à tour les questions et répondez-y dans la partie inférieure de la fenêtre.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur le questionnaire dans la liste des questionnaires et sélectionnez **Questionnaire d'évaluation (A remplir) > Soumettre les réponses**.

Après avoir consulté le contenu d'un questionnaire, vous pouvez en tant que répondant :

- Fermer le questionnaire sans y répondre.
- Demander le transfert du questionnaire vers un autre répondant
- Déléguer à une autre personne tout ou partie d'un questionnaire
- Accepter le questionnaire et y répondre

A partir du menu contextuel du questionnaire vous pouvez :

- déléguer tout ou partie d'un questionnaire à une tierce personne (si par exemple vous n'êtes pas la personne la plus apte à répondre à certaines questions).
- Faire une demande de transfert
- Fermer un questionnaire
  Après avoir coché les cases appropriées, plusieurs choix sont proposés au répondant :
  - Enregistrer : pour enregistrer les réponses apportées sans les envoyer immédiatement ; ceci permet de revenir au questionnaire pour le compléter a posteriori.
  - Soumettre les réponses pour validation.

> ☛ *Il est possible d'ouvrir et de fermer un questionnaire plusieurs fois avant de le soumettre.*

Remplir des check-lists d'évaluation

> ☛ *Les check-lists sont des questionnaires dédiés à la solution **Hopex Internal Control** et utilisés dans le cadre de l'exécution des contrôles.*

Des contrôles sont effectués périodiquement par les responsables de processus, pour vérifier que les processus opérationnels se sont bien déroulés et que leurs résultats sont conformes aux attentes.

En tant qu'utilisateur métier, vous devez pouvoir a accéder à ces contrôles, présentés sous forme de check-lists.

Pour remplir les check-lists qui vous sont adressées :

1. Dans la page d'accueil, cliquez **Mes tâches > Check-lists**.
2. Dans la liste qui apparaît, sélectionnez un objet à évaluer et dans le cadre inférieur, répondez aux questions de la check-list.
3. Sélectionnez un autre objet à évaluer et répondez aux questions.
4. Cliquez sur le bouton **Enregistrer**.
5. Une fois que vous avez répondu à toutes les questions, dans le menu contextuel de la check-list, cliquez sur **Questionnaire d'évaluation automatique (A remplir) > Terminer**.

> ☛ *Vous pouvez modifier vos réponses tant que vous n'avez pas cliqué sur **Terminer** dans le menu contextuel de la check-list.*

Si vous recevez un questionnaire par erreur, vous pouvez demander au responsable de la session de transférer le questionnaire à une autre personne.

Pour faire une demande de transfert :

- Cliquez sur l'icône d'un questionnaire et sélectionnez **Questionnaire d'évaluation (A remplir) > Demande de transfert**.
  Le questionnaire passe au statut "A réassigner".

  Un responsable est notifié par e-mail et doit réassigner le questionnaire à une autre personne.

> ☛ *Pour plus de détails sur l'exécution des contrôles, voir Exécuter les contrôles.*

CRÉER DES RISQUES ET CONTRÔLES

Créer un risque

Pour créer un risque dans le bureau du contributeur GRC:

- Dans la page d'accueil, cliquez sur **Créer un risque**.

  ☛ *Pour plus de détails sur les risques, voir Gérer les risques.*

Créer un contrôle

Pour créer un contrôle dans le bureau du contributeur GRC :

- Dans la page d'accueil, cliquez sur **Créer un contrôle**.

  ☛ *Pour plus de détails, voir Gérer les contrôles.*

GÉRER LES INDICATEURS CLÉS

> 🕮 *Un indicateur clé est une métrique utilisée par l'organisation pour alerter en cas d'exposition croissante à des risques dans différents secteurs de l'entreprise.*

Accéder aux indicateurs clés

Pour accéder aux indicateurs clés qui vous intéressent / pour lesquels vous devez saisir une valeur :

- Dans la barre de navigation, sélectionnez **Mes tâches > Indicateurs**.

> ☛ *Les indicateurs clés que vous pouvez visualiser sont ceux pour lesquels vous êtes autorisés à saisir une valeur. Voir Saisir une valeur d'indicateur clé.*

Une liste d'indicateurs apparaît, avec en colonnes les informations suivantes en lecture seule :

- **Statut courant**
  - Satisfaisant
  - Acceptable (avec avertissement)
  - Insatisfaisant
  - Critique
  - Non acceptable
- **Dernière mesure** : nombre de jours qui se sont écoulés depuis la dernière mesure
- **Temps avant défaillance** (en nombre de jours)

> 🕮 *Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".*

- **Valeur**
- **Limite haute** pour l'indicateur
- **Limite basse** pour l'indicateur

> ☛ *Dans les propriétés d'un indicateur clé, vous pouvez visualiser ses caractéristiques avancées ainsi que le graphique d'indicateur.*

Saisir une valeur d'indicateur clé

Pour saisir une valeur d'indicateur clé :

1. Voir Accéder aux indicateurs clés.
2. Ouvrez les propriétés d'un indicateur clé et sélectionnez l'onglet **Valeurs**.
3. Dans la section **Valeurs**, cliquez sur **Nouveau**.
4. Saisissez une valeur et cliquez sur **OK**.

Soumettre un plan d'action sur un indicateur clé

Pour créer et soumettre un plan d'action :

1. Voir Accéder aux indicateurs clés.

2. Ouvrez les propriétés d'un indicateur clé et sélectionnez l'onglet **Plans d'action**.
3. Cliquez sur **Nouveau** puis saisissez un commentaire ainsi que des dates prévisionnelles.
4. Passez la souris sur l'icône du plan d'action ainsi créé et sélectionnez **A soumettre > Proposer**.
5. Saisissez un commentaire puis cliquez sur **OK**.

RÉALISER UN BIA (BILAN D'IMPACT SUR L'ACTIVITÉ)

En tant que contributeur, vous pouvez être amené à réaliser des BIA (Bilans d'Impact sur l'Activité).

☛ *Cette fonctionnalité est disponible avec **Hopex BCM.***

Pour accéder à un BIA qui vous a été envoyé :

1. Dans l'arbre de navigation, sélectionnez **Mes tâches > Continuité d'activité**.
2. Dépliez la section **Bilans d'Impact sur l'Activité**.
   Tous les BIA qui vont son affectés apparaissent. Les BIA que vous avez fermés sont également disponibles pour que vous puissiez les rouvrir le cas échéant.
3. Ouvrez les propriétés du BIA qui vous concerne.
4. Répondez aux questions dans la section contenant la matrice BIA.
5. Cliquez sur le bouton **Terminer**.

PARTICIPER AUX PLANS DE CONTINUITÉ DE L'ACTIVITÉ

En tant que contributeur, vous pouvez être amené à participer aux Plans de Continuité de l'Activité

☛ *Cette fonctionnalité est disponible avec **Hopex BCM.***

Vous pouvez être amené à gérer des étapes de rétablissement :

- dans le cadre d'exercices de continuité de l'activité
- dans le cadre de crises

☛ *Les étapes de rétablissement doivent être menées à bien dans le cadre de Plans de Continuité de l'Activité spécifiques.*

Visualiser les PCA testés dans le cadre d'exercices

Vous pouvez être amené à participer au test de Plans de Continuité de l'Activité dans le cadre d'exercices en cours.

Pour les visualiser :

1. Dans l'arbre de navigation, sélectionnez **Mes tâches > Continuité d'activité**.
2. Dépliez la section **Plans de continuité d'activité testés dans le cadre d'exercices en cours**.

Cette liste affiche les PCA testés dans le cadre d'un exercice de continuité de l'activité en cours.

Visualiser les PCA déclenchés dans le cadre de crises

Vous pouvez être amené à participer à l'exécution de Plans de Continuité de l'Activité dans le cadre de crises.

Pour les visualiser :

1. Dans l'arbre de navigation :
   - (**Hopex GRC**) sélectionnez **Mes tâches > Continuité d'activité**.
   - (**Hopex Business Process Analysis**) Sélectionnez **Continuité > Tâches de continuité**.
2. Dépliez la section **Plans de continuité déclenchés dans le cadre de crises en cours**.

Cette liste affiche les PCA déclenchés dans le cadre d'une crise en cours.

ANNEXE - RÈGLES DE CALCUL

Dispositif de maîtrise du risque (DMR)

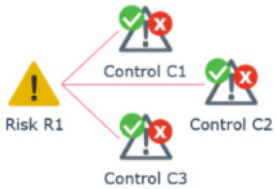
Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.

Contexte

Lorsqu'un répondant remplit un questionnaire d'évaluation des risques, **Hopex GRC** peut afficher une valeur dans la réponse à la question "Dispositif de maîtrise du risque" (DMR).

Une valeur est affichée si :

- le risque est atténué par un ou plusieurs contrôles.
- les contrôles atténuant ce risque ont déjà été évalués (ils disposent d'une valeur de niveau de contrôle agrégé).



Méthode de calcul

Le méthode de calcul se compose de deux étapes :

1) Calcul de la moyenne des niveaux de contrôle

```
Moyenne des niveaux de contrôle = Nb total de contrôles non
satisfaisants * 25 / Nb total de contrôles
```

2) Mise en correspondance du résultat obtenu (arrondi à l'entier supérieur) avec les valeurs internes du niveau de Dispositif de Maîtrise du Risque.

Dispositif de maîtrise du risque (sur Risque)	Valeur interne
Efficace	1
Perfectible	4
Peu efficace	9
Inefficace	16
Inexistant	25

☛ *Le niveau de Dispositif de Maîtrise du Risque affiché correspond à la valeur interne la plus proche de la moyenne précédemment calculée.*

Exemple : le Dispositif de Maîtrise du Risque est jugé "Peu efficace" si la moyenne des niveaux de contrôle = 10.

Exemple de calcul

Contrôle	Niveau de contrôle agrégé	Valeur du niveau de contrôle
C1	90%	1
C2	45%	0
C3	0%	0

Moyenne des niveaux de contrôle = 2*25/3 = 16,6 -> arrondi à 17.

☛ *Les deux contrôles C2 et C3 sont jugés non satisfaisants (car < 90%).*

Le Dispositif de Maîtrise du Risque est jugé inefficace (car 16 est la valeur interne la plus proche de 17).

Risque inhérent

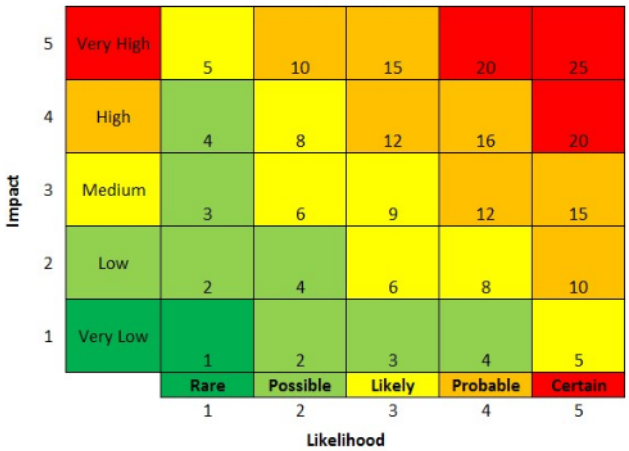
Le risque inhérent (ou risque brut) désigne le risque auquel l'organisation est exposée en l'absence de mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque.

Méthode de calcul

Risque inhérent = Impact * Probabilité

Valeurs possibles

- Très bas (1)
- Bas (4)
- Moyen (9)
- Elevé (16)
- Très élevé (25)



Risque résiduel

Le risque résiduel (risque net) désigne le risque auquel l'organisation reste exposée une fois que le management a traité le risque.

Méthode de calcul

Le risque résiduel est calculé à partir du risque inhérent (Impact * Probabilité) et du dispositif de Maîtrise de Risque.

Valeurs possibles

- Très bas (1)
- Bas (16)
- Moyen (81)
- Elevé (256)
- Très élevé (625)

Risque inhérent						
	Très élevé	Moyen	Moyen	Elevé	Elevé	Très élevé
	Elevé	Bas	Moyen	Moyen	Elevé	Elevé
	Moyen	Bas	Bas	Moyen	Moyen	Moyen
	Bas	Très bas	Bas	Bas	Bas	Bas
	Très bas	Très bas	Très bas	Très bas	Très bas	Très bas
		Très élevé	Elevé	Moyen	Bas	Très bas
		Dispositif de Maîtrise de Risque				

Calcul du RTO (Recovery Time Objective)

📖 *Le RTO (Recovery Time Objective) détermine le temps maximum tolérable nécessaire pour remettre les systèmes critiques en fonctionnement, éventuellement en mode dégradé.*

☛ *Pour plus de détails, voir Visualiser les résultats calculés d'un BIA.*

L'algorithme :

- additionne le poids des réponses des types d'impact pour chaque temps d'arrêt, en partant du temps d'arrêt le plus court jusqu'au plus long
- compare la somme des poids au seuil du RTO.

Le seuil du RTO est défini pour chaque temps d'arrêt. Il s'agit de la valeur possible maximum des réponses du BIA moins 30%.

Si le temps d'arrêt pour lequel la somme des valeurs des réponses est plus grand que le seuil du RTO, c'est ce temps d'arrêt qui devient le RTO calculé.

Valeurs maximales (« critiques »)

	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
Somme →		40		40		40		40		40		40

Seuil du RTO (pour chaque temps d'arrêt) = Somme des valeurs maximales - 30%
Exemple ci-dessus (issu du modèle standard) : 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 est supérieur à la valeur du seuil du RTO
> Le RTO est de « 1 jour ».

Calcul de l'impact sur l'activité

L'impact sur l'activité est calculé à partir des réponses apportées dans la matrice du BIA.

☛ *Pour plus de détails, voir Définir un Bilan d'Impact sur l'Activité.*

L'algorithme calcule l'impact sur l'activité de la manière suivante :

Si RTO = ...	**... Impact sur Activité =**
12 heures ou 1 jour	Critique
2 jours ou une semaine	Moyen
Autres valeurs	Faible

GLOSSAIRE GRC

action

Une action est incluse dans un plan d'action et représente une transformation ou un traitement dans une organisation ou un système.

activité d'audit

Une activité d'audit est un élément d'une mission d'audit qui peut porter sur un ensemble de processus, d'applications, de risques ou de contrôles à auditer dans un département de l'entreprise.

appétence au risque

L'appétence au risque est le niveau de risque qu'une organisation est prête à accepter pour atteindre ses objectifs, avant toute mesure prise pour atténuer le risque.

application

Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.

approbateur d'incident

Rôle utilisé dans le cadre des workflows standards pour l'approbation des incidents.

article (de texte de référence)

Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.

audit interne

L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité (source : IFACI).

base de données

Une base de données permet de spécifier la structure de stockage logique ou physique des données.

bibliothèque

Une bibliothèque est un regroupement d'objets qui permet de découper le contenu d'un référentiel Hopex en plusieurs parties indépendantes. Deux objets appartenant à des bibliothèques différentes peuvent ainsi avoir le même nom.

cadre de politique d'entreprise

Un cadre de politique d'entreprise constitue un ensemble de politiques d'entreprise. Les cadres de politique d'entreprise peuvent contenir des sections.

cadre réglementaire

Un cadre réglementaire représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.

calendrier

Un calendrier est divisé en périodes de calendrier.

calendrier

Un calendrier est divisé en périodes de temps appelées périodes de calendrier. Les calendriers peuvent servir dans le cas des campagnes d'évaluation, de la génération de rapports, ainsi que pour planifier les missions d'audit/ de test.

calendrier de pilotage

Un calendrier de pilotage permet d'effectuer des actions récurrentes à des dates d'échéances prédéfinies. On peut par exemple l'utiliser pour envoyer des rappels à la personne responsable d'un plan d'action afin qu'elle renseigne le taux d'avancement de ce plan d'action. On peut aussi utiliser un calendrier

de pilotage pour déclencher automatiquement le lancement de sessions d'évaluation à des échéances régulières,...

campagne d'évaluation

Une campagne d'évaluation permet de créer et de planifier plusieurs sessions d'évaluation sur une période donnée.

caractéristique évaluée

Une caractéristique évaluée définit ce que l'évaluation cherche à évaluer. Elle peut être associée à une MetaClasse et précisément à l'un de ses MetaAttributs, par exemple : Metaclasse Risque, MetaAttribut: Criticité.

catégorie d'indicateur clé

La catégorie d'indicateur clé détermine la façon dont les valeurs de l'indicateur sont interprétées, de façon à obtenir le statut de l'indicateur et le temps avant défaillance.

catégorie de processus

Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.

centre de données

Un centre de données est un site physique qui regroupe des installations informatiques chargées de stocker et de distribuer des données à travers un réseau interne ou via un accès Internet.

conséquence de risque

Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.

constat

Les constats d'audit sont les résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit. Les constats d'audit peuvent indiquer la conformité ou la non-conformité aux critères d'audit, ou des opportunités d'amélioration.

contrat

Un contrat est un accord entre l'organisation et un fournisseur.

contrôle

Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.

correspondant Contrôle

Le correspondant Contrôle est responsable de l'évaluation et de l'exécution des contrôles de son périmètre ainsi que de mise en œuvre des plans d'action relatifs à ces contrôles.

correspondant Risque

Le correspondant Risque est responsable de l'évaluation des risques de son périmètre, ainsi que de la mise en œuvre des plans d'action relatifs à ces risques.

déclarant d'incident

Le déclarant d'incident est responsable de la création d'incidents de son périmètre.

département

Un département représente un élément de la structure d'une entreprise tel qu'une direction ou un service. Il est défini à un niveau plus ou moins fin en fonction de la précision que l'on doit fournir sur l'organisation. Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial.

devise centrale

La devise centrale est la devise retenue par l'entreprise comme devise de référence.

devise locale

Une devise locale est définie pour chaque utilisateur. Il s'agit par défaut de la devise centrale.

dispositif de contrôle et de risque

Un dispositif de contrôle est constitué d'un ensemble de contrôles qui permettent d'assurer la prévention et la maîtrise des risques encourus par l'entreprise, l'application de règles de fonctionnement internes, le respect d'une loi ou d'une réglementation en vigueur, ou l'atteinte d'un objectif stratégique de l'entreprise. Exemples : le dispositif de contrôle de la Qualité, le dispositif de contrôle de gestion, le dispositif d'audit interne.

dispositif de maîtrise du risque

Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.

document métier

Un document métier est un document dont le contenu est indépendant du référentiel HOPEX. Ce document peut être un fichier MS Word, MS Powerpoint ou autres. Un rapport (MS Word) généré sur un objet peut devenir un document métier.

entité

Une entité représente une personne ou un groupe de personnes qui interviennent dans les processus ou dans le système d'information de l'entreprise.

entité

Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.

évaluation

L'évaluation est un mécanisme qui permet de lancer des questionnaires à une population identifiée afin d'obtenir des estimations (qualitatives ou quantitatives) sur des objets identifiés.

exigence

Une exigence est un besoin ou une attente formulés explicitement, imposés comme une contrainte à respecter dans le cadre d'un projet de certification, d'organisation ou de modification du système d'information d'une entreprise.

facteur de risque

Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.

fiche de travail

Une fiche de travail est constituée de points à vérifier sur un sujet donné au cours d'une activité d'audit.

fournisseur

Un fournisseur est un acteur externe de type "Fournisseur".

fraîcheur de l'évaluation

La fraîcheur de l'évaluation est le temps écoulé (en nombre de jours) depuis que la dernière valeur de l'indicateur clé a été saisie.

gain

Un gain est la conséquence financière positive d'un incident.

incident

Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.

indicateur

Un indicateur est une grandeur mesurable servant à fournir des indications sur l'atteinte d'un objectif, l'impact d'un facteur de risque, la fréquence ou l'impact d'un risque, l'efficacité d'un contrôle, etc.

indicateur clé

Un indicateur clé est une métrique utilisée par l'organisation pour alerter en cas d'exposition croissante à des risques dans différents secteurs de l'entreprise.

installation

Une installation est un modèle de site d'intérêt pour l'entreprise (par exemple : une usine ou une agence).

installation logicielle

Une Installation de logiciel sur un site permet d'offrir un ensemble de fonctionnalités à différentes populations d'utilisateurs.

ligne métier

Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.

logique d'interprétation d'indicateur

Une logique d'interprétation d'indicateur contient la logique de calcul du statut de l'indicateur, le temps avant défaillance, ainsi que la liste des statuts dans lesquels l'indicateur peut se trouver.

macro-incident

Un macro-incident est un incident qui a des incidences sur plus d'un métier ou d'une société d'un même groupe.

méthode d'agrégation

Une méthode d'agrégation est une opération mathématique réalisée sur les valeurs agrégées de l'indicateur clé, de manière à calculer la valeur de ce dernier ainsi que son statut.

métrique

Une métrique sert à fournir des indications quantitatives sur la valeur d'une grandeur (par exemple le niveau de prévention d'un risque).

mission d'audit

Une mission d'audit est une mission affectée à une équipe d'auditeurs internes dans le cadre d'un plan d'audit.

mission de test

Une mission de test est une mission assignée à un contrôleur dans le cadre d'un plan.

modèle d'évaluation

Un modèle d'évaluation sert de modèle pour la construction de campagnes et de sessions d'évaluations.

Le modèle d'évaluation définit le périmètre de l'évaluation, le modèle de questionnaire à utiliser, éventuellement les schémas d'agrégation à appliquer pour l'interprétation des résultats globaux.

modèle de questionnaire

Un modèle de questionnaire représente la définition du contenu d'un questionnaire.

niveau de contrôle

Le niveau de contrôle permet de caractériser le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour atténuer le risque.

Il s'agit du pourcentage de nœuds d'évaluation (objets évalués dans chaque contexte) ayant obtenu un niveau de contrôle Satisfaisant au cours de la dernière évaluation directe ou par campagne.

objectif

Un objectif est un but que l'on cherche à atteindre ou la cible visée pour un processus ou une opération. Il permet de mettre en évidence les points que l'on veut améliorer pour ce processus ou cette opération.

obligation

Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.

opération

Une opération est une étape élémentaire d'un processus. Elle correspond à l'intervention d'un acteur de l'organisation.

période

Une période correspond à l'exercice au cours duquel les missions d'audit sont réalisées. Elle permet de regrouper chronologiquement plusieurs plans d'audit.

période d'agrégation

La période d'agrégation est la période au cours de laquelle les valeurs de l'indicateur clé sont agrégées, de manière à calculer sa valeur et son statut.

période de calendrier

Une période de calendrier est une division d'un calendrier.

personne

Une personne est définie par son nom et son adresse électronique. Elle peut accéder à une application dès lors qu'on lui attribue un identifiant de connexion. Un ou plusieurs rôles métiers peuvent également lui être assignés.

perte

Une perte est la conséquence financière négative d'un événement.

phase d'entreprise

Une phase d'entreprise est une phase passée, courante ou future d'une entreprise.

plan d'action

Un plan d'action est constitué d'une série d'actions, avec pour objectif de réduire les risques et les événements ayant un impact négatif sur l'activité de l'entreprise.

plan de test

Le plan de test est la description du champ de l'audit attendu et de sa conduite. Il est réalisé conformément à des normes d'audit. Il comprend la description de l'approche d'audit ainsi que le planning. Il se compose de plusieurs missions de test durant une période donnée.

politique d'entreprise

Une politique d'entreprise est un document interne émis par une organisation (code de bonne pratique, mesure de sécurité, etc.).

processus

Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.

produit

Un produit représente un ou plusieurs articles, objets, biens ou services, résultat d'une activité agricole, industrielle ou de service, qui sont proposés par une entreprise.

profil

Un profil définit l'accès à des fonctionnalités de l'application ainsi qu'un niveau d'intervention dans le workflow et le processus de validation.

programme d'activité

Un programme d'activité est un modèle d'activité, portant les caractéristiques principales d'une activité d'audit à effectuer.

programme de mission

Un programme de mission est un modèle de mission portant les caractéristiques principales d'une mission d'audit.

provision

Une provision est un montant qui diminue le résultat pour faire face à un risque ou une charge incertaine. Plusieurs provisions peuvent concerner un seul et même risque.

quasi-incident

Un quasi-incident est un incident qui ne s'est traduit ni en dommages corporels ni en dommages matériels mais qui en avait le potentiel.

questionnaire

Un questionnaire d'évaluation est une liste de questions portant sur un objet particulier et adressée à des utilisateurs.

recommandation

Une recommandation décrit ce qui doit être réalisé pour corriger une non-conformité détectée durant l'audit.

récupération

Une récupération est une somme qui dans certaines circonstances vient réduire le montant des pertes liées au risque opérationnel. Elle permet de récupérer une partie des sommes engagées dans l'événement.

redondance de contrôles

Une redondance de contrôles formalise le fait que plusieurs contrôles sont redondants. Ce peut être, par exemple, parce qu'ils ont été successivement mis en place pour couvrir un même risque dans le cadre de réglementations différentes.

règle d'agrégation

Une règle d'agrégation permet de calculer les valeurs d'une caractéristique d'évaluation parente à partir d'une ou plusieurs caractéristiques d'évaluation filles. Quelques règles sont prédéfinies, par exemple : max, min, sum, average.

règle de notation

Une règle de notation détermine comment les réponses à un questionnaire alimentent les caractéristiques de l'objet évalué.

réglementation ou règlement interne

Une réglementation ou un règlement interne représente un ensemble de directives contraignantes ou non, définies par un gouvernement dans le cadre d'une loi, par un groupement professionnel sous forme de bonnes pratiques ou en interne par une organisation.

répondant

Un répondant est une personne de l'entreprise interrogée dans le contexte d'une évaluation. Cette personne doit compléter le questionnaire d'évaluation et le renvoyer.

Risk Manager

Le Risk Manager est responsable de l'exécution des tâches suivantes concernant les risques de son domaine de responsabilité : identifier les risques, réaliser des évaluations directes, gérer les campagnes d'évaluation, définir des plans d'action, analyser et suivre la création de rapports.

risque

Un risque est un danger plus ou moins probable auquel est exposée une organisation.

risque inhérent

Le risque inhérent (ou risque brut) est le risque auquel une entité est exposée en l'absence de mesures correctives par le management pour en modifier la probabilité d'occurrence ou l'impact, par opposition au risque résiduel.

risque matérialisé

Un risque qui s'est matérialisé est un risque pour lequel un incident s'est produit.

risque prévisionnel

Le risque prévisionnel représente la projection du risque résiduel sur l'année à venir.

risque résiduel

Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.

rôle

Un rôle est l'association d'un profil à un utilisateur dans un contexte organisationnel précis.

schéma d'agrégation

Une schéma d'agrégation est une suite d'étapes qui permettent de consolider les résultats d'une évaluation en fonction de règles d'évaluation prédéfinies.

section (de texte de référence)

Une section est une citation d'un texte de référence, qui n'est associée à aucune obligation légale et qui contient d'autres sections ou articles.

serveur

Un serveur est une ressource informatique matérielle, pouvant disposer d'une Base de données et sur laquelle des Applications peuvent s'exécuter.

serveur déployé

Un serveur (déployé) est une ressource informatique sur laquelle des applications s'exécutent.

session d'évaluation

Une session d'évaluation est une évaluation lancée sur un laps de temps déterminé. La publication de la session d'évaluation a pour effet d'envoyer un formulaire d'évaluation contenant les questions aux utilisateurs ciblés.

site

Un site est un lieu géographique où est implantée l'entreprise. Les sites peuvent être des sites-types tels que le siège, l'agence, l'usine, ou des lieux géographiques précis comme l'agence de Marseille, l'usine de Poissy, etc.

société

Une société est une personne morale.

statut d'indicateur

Le statut d'un indicateur permet de déterminer si une alerte doit être déclenchée. L'indicateur est calculé automatiquement en se basant sur les dernières valeurs de l'indicateur, la période d'agrégation et la méthode d'agrégation.

taux d'exécution

Le taux d'exécution est le pourcentage d'objets contextes du périmètre du contrôle inclus dans la dernière campagne d'exécution de contrôles.

taux de conformité

Le taux de conformité est le pourcentage de contrôles jugés satisfaisants.

technologie logicielle

Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.

temps avant défaillance

Le temps avant défaillance est le nombre de jours devant s'écouler avant passage de l'indicateur clé en statut "Non acceptable".

texte de référence

Un texte de référence est un texte qui entre dans l'une des catégories suivantes : réglementations (textes de lois qui peuvent entraîner des pénalités s'ils ne sont pas respectés), standards ou normes.

thème d'audit

Un thème d'audit est un regroupement d'activités d'audit portant sur un même sujet. Les thèmes d'audit peuvent se décomposer en sous-thèmes d'audit.

type de contrôle

Un type de contrôle permet de classifier les contrôles mis en oeuvre dans l'entreprise conformément à des standards sectoriels ou réglementaires (Cobit, etc.).

type de risque

Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.

HOPEX Internal Control

Guide d’utilisation

Bizzdesign

HOPEX Aquila 6.2

SOMMAIRE

Sommaire

A PROPOS DE LA GESTION DES CONTRÔLES

Hopex Internal Control est une solution de gestion du contrôle interne qui couvre les différentes phases du contrôle interne. Cette solution permet de :

- ✓ définir des dispositifs de contrôle interne avec la mise en place d'une bibliothèque de contrôles
- ✓ exécuter des contrôles
- ✓ évaluer les contrôles, directement, par le biais de campagnes d'évaluation ou de missions de tests
- ✓ gérer votre bibiliothèque réglementaire et la mise en conformité informatique
- ✓ gérer les défaillances et plans d'action

Hopex Internal Control s'adresse aux responsables du contrôle interne, contrôleurs internes, et responsables de catégorie de processus. Une interface personnalisée en fonction du profil de connexion accompagne chacun tout au long de la mise en œuvre des dispositifs de contrôle interne.

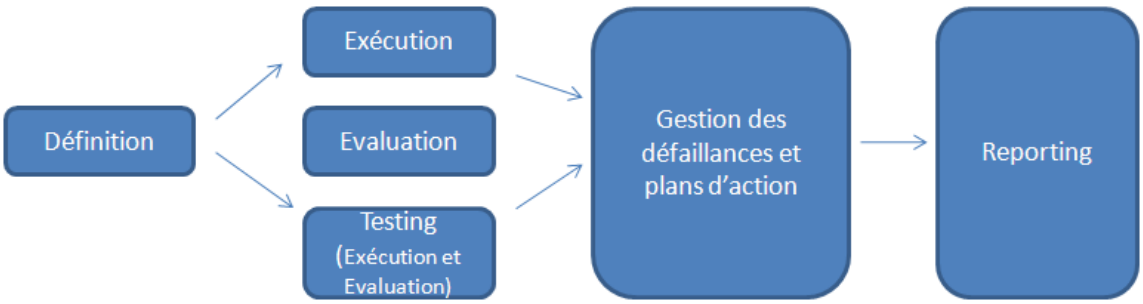
- ✓ Processus du contrôle interne
- ✓ Profils de gestion des contrôles

PROCESSUS DU CONTRÔLE INTERNE

Le contrôle interne consiste à vérifier que les contrôles effectués durant l'exécution des processus de l'entreprise sont réalisés correctement et qu'ils sont efficaces.

Hopex Internal Control couvre les différentes phases du contrôle interne :

- Définition d'une bibliothèque de contrôles
- Exécution des contrôles
- Evaluation des contrôles
- Testing des contrôles
- Gestion des défaillances et des plans d'action



La définition du registre de contrôles est une condition préalable aux activités d'exécution et d'évaluation des contrôles.

L'exécution et l'évaluation des contrôles peuvent être effectuées de manière indépendante.

☛ *Les fonctionnalités de reporting sont disponibles à tout moment, de manière globale, ou pour chaque étape du contrôle interne.*

Définition d'un registre de contrôles

Hopex Internal Control permet aux responsables du contrôle interne :

- d'identifier les contrôles
- de contextualiser les contrôles dans le référentiel d'entreprise, c'est-à-dire de les relier aux catégories de processus, processus et entités appropriés.

Voir Gérer les contrôles.

Exécution des contrôles

Des contrôles sont exécutés régulièrement par la hiérarchie pour s'assurer que les contrôles de premier niveau sont réalisés correctement. **Hopex Internal Control** permet de :

- créer des questionnaires appelés check-lists
- définir à intervalle régulier des campagnes d'exécution de contrôles
- suivre et consolider les résultats de l'exécution des contrôles à partir de rapports.

> ☛ *La solution **Hopex Internal Control** ne concerne pas les contrôles de premier niveau réalisés par les opérationnels durant l'exécution des processus de l'entreprise.*

Voir Exécuter les contrôles.

Evaluation des contrôles

L'évaluation de la pertinence des contrôles en termes de conception et d'efficacité peut être réalisée grâce à des :

- campagnes d'évaluation via l'envoi de questionnaires
  Voir Campagnes d'évaluation.
- évaluation directe
  Voir Evaluer les contrôles
- missions de test de contrôles organisées par le service du contrôle interne
  Voir Tester les contrôles

Gestion des défaillances et des plans d'action

Les défaillances peuvent être identifiées à partir des questionnaires d'évaluation des contrôles ou renseignées directement dans la solution.

La résolution des défaillances est formalisée par la mise en oeuvre de plans d'action. Des rapports permettent d'assurer un suivi efficace des activités du contrôle interne.

Voir Gérer les défaillances et plans d'action.

PROFILS DE GESTION DES CONTRÔLES

Pour se connecter à Hopex, voir **Hopex Common Features**, "Le bureau Hopex", "Accéder à Hopex (Web Front-End)".

Profils	Bureau	Tâches
Directeur du contrôle interne (ou Manager GRC)	Hopex GRC	- Possède tous les droits sur les workflows, menus et objets de la solution. - Valide les campagnes - Prépare les plans de test - Valide les plans d'action
Contrôleur interne (ou Manager GRC)	Hopex GRC	- Définit les contrôles - Prépare les campagnes - Exécute les missions de test (élabore le programme de travail, crée des défaillances et plans d'action) - Valide et suit les plans d'action
Contributeur GRC (simplifié)	Contributeurs GRC	- Remplit les check-lists d'exécution des contrôles - Répond aux questionnaires d'évaluation - Définit et élabore les plans d'action (et crée les défaillances) Voir Bureau des contributeurs GRC.

☛ *Pour plus de détails, voir Accéder au bureau GRC.*

GÉRER LES CONTRÔLES

Hopex GRC permet de créer un registre de contrôles et de relier ces contrôles à des objets de leur environnement. Ceci permet de les positionner dans leur contexte métier. Cette "contextualisation" permet aux responsables du contrôle interne de définir des contrôles adaptés et de conduire par la suite des évaluations pertinentes.

CRÉER UN CONTRÔLE

Pour créer un contrôle :

1. Dans la barre de navigation, cliquez sur **Contrôles**.
2. Cliquez sur **Nouveau**.

   ☛ *Vous pouvez également créer un contrôle depuis la page d'accueil (zone d'**Accès rapide > Actions > Créer un contrôle**).*

3. Dans l'assistant de création, saisissez :
   - le **Nom**
   - la **Nature du contrôle**
   - le **Mode d'exécution**
   - une **Description**

     ☛ *Pour plus de détails sur les caractéristiques, voir Caractéristiques d'un contrôle.*

Le contrôle créé apparaît dans la liste des contrôles.

Vous pouvez compléter les caractéristiques à partir de la page de propriétés.

CARACTÉRISTIQUES D'UN CONTRÔLE

☛ *Pour accéder aux contrôles, voir Accéder aux contrôles.*

Caractéristiques générales

Code

Le code permet d'identifier le contrôle de manière unique.

Contrôle clé

Permet de définir si le contrôle est un contrôle majeur ou non.

Statut

- Version préliminaire
- Validé

☛ *Le statut est à saisir manuellement.*

Propriétaire

Le propriétaire du contrôle est par défaut son créateur.

☛ *Le propriétaire ne possède pas de fonction particulière.*

Nature de contrôle

Cette caractéristique permet de préciser la nature du contrôle. Vous pouvez choisir parmi les trois types principaux de contrôle interne :

- "Correction"
- "Détection"
- "Prévention"

Mode d'exécution

Cette caractéristique permet de préciser de quelle manière le contrôle est effectué :

- "Automatique"
- "Manuel"
- "Semi-automatique"

Coût opérationnel

Cette caractéristique permet d'indiquer une évaluation du coût du contrôle.

Description et Objectif de contrôle

Vous pouvez saisir un commentaire et/ou un texte spécifique décrivant l'objectif recherché dans la mise en place du contrôle.

Vue d'ensemble d'un contrôle

☛ *Voir Accéder aux contrôles.*

La page **Vue d'ensemble** donne accès à:

- une carte du contrôle, qui fournit un aperçu des principales caractéristiques du contrôle.

  ☛ *Pour plus de détails sur les cartes d'objets, voir Carte d'un objet, dans la section "Plateforme - Fonctionnalités communes".*

- des informations calculées, sous forme de tableau de bord

Fiche d'identification

Une fiche d'identification du contrôle rappelle les caractéristiques principales :

- **Code**

  ☛ *Voir Code.*

- **Description**

  ☛ *Voir Description et Objectif de contrôle.*

- **Propriétaire**

  ☛ *Voir Propriétaire.*

- **Mode d'exécution**

  ☛ *Voir Mode d'exécution.*

- **Nature**

  ☛ *Voir Nature de contrôle.*

- **Clé**

  ☛ *Voir Contrôle clé.*

Tableau de bord

Dernière évaluation

Cet indicateur permet de savoir quand la dernière évaluation a été réalisée.

Dernier taux de conformité

Le taux de conformité concerne les check-lists d'exécution de contrôles. Pour plus de détails sur cette fonctionnalité, voir Exécuter les contrôles.

📖 *Le taux de conformité est le pourcentage de contrôles jugés satisfaisants.*

Défaillances non traitées

Les défaillances non traitées sont les défaillances pour lesquelles le plan d'action n'est pas terminé.

Pour plus de détails, voir Gérer les défaillances et plans d'action.

Niveau de contrôle

Le niveau de contrôle concerne l'évaluation des contrôles. Pour plus de détails, voir Afficher les résultats d'évaluation de contrôle.

Le niveau de contrôle est le pourcentage de nœuds d'évaluation (objets évalués dans chaque contexte) ayant obtenu un niveau de contrôle Satisfaisant au cours de la dernière évaluation directe ou par campagne.

> Si le contrôle est évalué dans 2 contextes (par exemple 2 catégories de processus) et que seule une des deux évaluations a obtenu le niveau de contrôle " Satisfaisant ", le niveau de contrôle est de 50%.

Niveau de contrôle = Conception du contrôle (IC) * Efficacité du contrôle (IC).

Responsabilités concernant les contrôles

Voir aussi : Accéder aux contrôles.

Hopex GRC permet de définir les responsabilités de chacun par rapport à un contrôle via la matrice RACI :

- Réalisateur
- Autorité
- Consulté
- Informé

Niveaux de responsabilité

Les niveaux de responsabilité de type RACI sont les suivants :

Responsabilité	Explication
Réalisateur	Chargé de la réalisation des actions prévues.
Autorité	Rend compte de l'avancement des actions prévues et prenant des décisions. Il n'existe qu'une seule "Autorité".
Consulté	Consulté prioritairement avant une action ou décision.
Informé	Acteur devant être informé après une action ou décision.

Spécifier les réalisateurs du contrôle

Dans le cadre de l'évaluation et de l'exécution des contrôles, les répondants des questionnaires sont les ***Réalisateurs*** du contrôle.

☛ *Voir la section correspondant à la logique des répondants dans les paragraphes consacrés aux modèles d'évaluation de contrôle : Pré-requis à l'évaluation des contrôles.*

☛ *Voir aussi : Campagnes d'évaluation.*

Pour spécifier le réalisateur d'un contrôle dans une entité donnée :

1. Dans la page de propriétés du contrôle, dépliez la section **Responsabilités**.

   ☛ *Pour accéder aux contrôles, voir Lister tous les contrôles.*
2. Sélectionnez l'onglet **Réalisateur**.
3. Cliquez sur le bouton **Nouveau**.
4. Sélectionnez une personne dans la liste déroulante prévue à cet effet.

   ☛ *Le rôle métier "Réalisateur de contrôle" est rappelé.*
5. (optionnel) Sélectionnez l'entité dont la personne est responsable.
6. Cliquez sur **OK**.

   ☛ *Veillez à ce qu'un e-mail soit correctement renseigné à côté du nom de la personne.*

   ☛ *Vous avez la possibilité de relier plusieurs réalisateurs.*

Périmètre d'un contrôle et risques associés

Pour spécifier le périmètre d'un contrôle :

- Dans la page **Caractéristiques** des propriétés d'un contrôle, dépliez la section **Périmètre.**
  Vous pouvez y relier différents types d'objets :
  - Catégories de processus
  - Processus
  - Opérations
  - Entités
  - Applications
  - Comptes
  - Types de contrôle

Pour spécifier les risques d'un contrôle :

- Dans la page **Caractéristiques** des propriétés d'un contrôle, dépliez la section **Risques**.

Application de la réglementation et des politiques d'entreprise

Pour visualiser les éléments de réglementation et de politiques d'entreprise qui sont reliés à un contrôle :

1. Voir Accéder aux contrôles.

2. Dans la page **Caractéristiques** des propriétés d'un contrôle, dépliez la section **Application de la réglementation et des politiques d'entreprise**.

Des onglets vous permettent de visualiser les objets reliés :

- Obligations

  Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.

- Articles

  Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.

- Politiques d'entreprise

  ☛ *Pour plus de détails, voir Gérer la conformité.*

Plans d'actions concernant les contrôles

Pour spécifier des plans d'action concernant un contrôle :

❱ Dans les propriétés du contrôle, sélectionnez la page **Plans d'action.**

Vous pouvez :

- définir des plans d'action directement sur le contrôle.
- visualiser les plans d'action concernant les défaillances associées à ce contrôle.

  ☛ *Pour plus de détails, voir Gérer les défaillances et plans d'action.*

Rapport concernant les contrôles

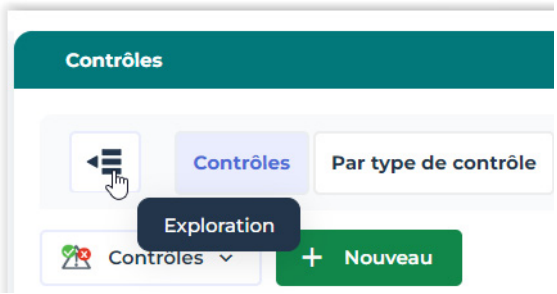
Voir Rapport d'environnement d'un contrôle.

Explorer l'environnement d'un contrôle

Pour explorer les objets de l'environnement d'un contrôle :

1. Voir Accéder aux contrôles.

2. Dans la liste des contrôles, cliquez sur le bouton **Exploration**.

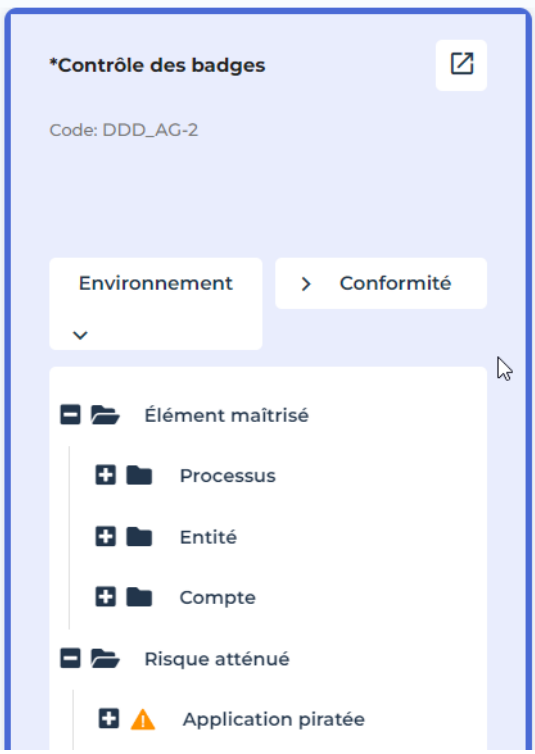


Des cartes apparaissent pour chaque contrôle.

3. Passez la souris sur une carte et cliquez sur **Environnement**.

Les éléments de l'environnement du contrôle s'affichent dans des arborescences. Il s'agit du périmètre étendu du contrôle.

- Éléments de l'environnement
- Éléments de l'environnement de conformité / concernant l'application de la réglementation.


*Contrôle des badges
Code: DDD_AG-2
Environnement
Conformité
Élément maîtrisé
Processus
Entité
Compte
Risque atténué
Application piratée

ACCÉDER AUX CONTRÔLES

Vous pouvez accéder aux contrôles par différentes listes, qui permettent de les classer selon différents critères.

Par défaut, les contrôles sont visibles par tous. En revanche, vous ne pouvez modifier que les contrôles qui sont rattachés à votre entité de référence ou à une de ses sous-entités.

> Si, de par votre assignation, vous êtes relié à l'entité "France", vous ne pouvez pas modifier les contrôles qui ont pour contexte l'entité "Monde".
>
> En revanche, si vous êtes relié à l'entité "Monde", vous pouvez modifier les contrôles qui ont pour contexte l'entité "France".

Lister tous les contrôles

Pour lister tous les contrôles :

- Dans la barre de navigation, cliquez sur **Contrôles**.

Accéder aux contrôles orphelins

Pour accéder aux contrôles qui n'atténuent aucun risque et qui ne sont reliés à aucun élément de l'organisation :

1. Voir Lister tous les contrôles
2. Dans la liste déroulante, sélectionnez **Contrôles orphelins**.

> ☛ *Pour définir correctement un contrôle, reliez-le à un risque et assurez-vous d'avoir défini le périmètre de ce risque.*

Accéder aux contrôles par incidents

Pour accéder aux contrôles qui atténuent des risques matérialisés par un ou plusieurs incidents :

1. Voir Lister tous les contrôles
2. Dans la liste déroulante, sélectionnez **Contrôles avec incidents**.

> ☛ *Un risque est considéré comme matérialisé lorsqu'il est relié à un incident qui se trouve dans un statut autre que Projet ou Rejeté.*

CONTEXTUALISER LES CONTRÔLES

Un même contrôle peut être évalué dans le cadre de contextes différents (par exemple catégories de processus, processus ou entités).

Pour permettre cette évaluation, vous devez "contextualiser" les contrôles, c'est-à-dire les relier à des objets de contexte.

Vous devez ***relier les contrôles à des risques, eux-mêmes reliés à des catégories de processus, processus ou entités***.

☛ *Vous pouvez également **relier les contrôles à des entités via le lien indirect "Contrôle->Processus->Entité"**, c'est-à-dire :*

- *Relier des catégories de processus ou processus aux entités de l'organisation.*
- *Relier les contrôles à ces catégories de processus et processus.*

EVALUER LES CONTRÔLES

Les contrôles sont évalués en termes de conception et d'efficacité.

L'évaluation peut être effectuée :

- directement sur les contrôles (évaluation à dire d'expert)
- via des questionnaires (contributeur GRC).

Hopex GRC permet également aux contrôleurs internes et auditeurs de répondre à des questionnaires sur site. Pour plus de détails, voir Tester les contrôles.

☛ *Ce chapitre explique comment lancer les évaluations. Pour les paramétrer, voir Assessment Templates dans la documentation **Hopex Power Studio - Assessment**.*

TYPES D'ÉVALUATION DES CONTRÔLES

☛ *Une évaluation est destinée à donner des valeurs, dans un contexte précis, aux différentes caractéristiques d'un contrôle.*

Évaluation directe ou par campagne

Évaluation directe

Le Manager GRC peut spécifier les valeurs des caractéristiques de deux manières :

- dans les propriétés d'un contrôle : voir Évaluer un contrôle.
- via un tableau d'évaluation multiple : voir Évaluer plusieurs contrôles simultanément.

Évaluation par campagne

Les valeurs des caractéristiques peuvent être recueillies via un questionnaire d'évaluation envoyé à des destinataires appropriés : voir Lancer une campagne d'évaluation.

Modèles d'évaluation pour les contrôles

Hopex vous permet d'évaluer les contrôles selon deux perspectives :

- Évaluation des contrôles par entité
- Évaluation des contrôles par entité et texte de référence.

☛ *Voir Pré-requis à l'évaluation des contrôles pour plus de détails sur ces modèles d'évaluation.*

PRÉ-REQUIS À L'ÉVALUATION DES CONTRÔLES

Évaluation des contrôles par entité

Le modèle "Évaluation des contrôles par entité " permet d'évaluer les contrôles dans le contexte des entités et catégories de processus/processus sur la base des critères suivants :

- Conception
- Efficacité

Contextes de l'évaluation

Les contrôles sont évalués dans le contexte d'entités, catégories de processus, processus et opérations.

Pré-requis

Avant de lancer une évaluation de contrôles, vous devez avoir préparé l'environnement de travail.

Assurez-vous d'avoir :

- relié les contrôles à des catégories de processus et processus (indirectement via des risques, ou directement)
- relié les catégories de processus et processus aux entités de l'organisation (directement ou indirectement via la catégorie de processus).

  ☛ *Voir Contextualiser les contrôles.*
- défini des répondants.

  ☛ *Voir :*

  - *Pré-requis à l'évaluation des contrôles*
  - *Spécifier les répondants*
- spécifié un e-mail pour chaque répondant

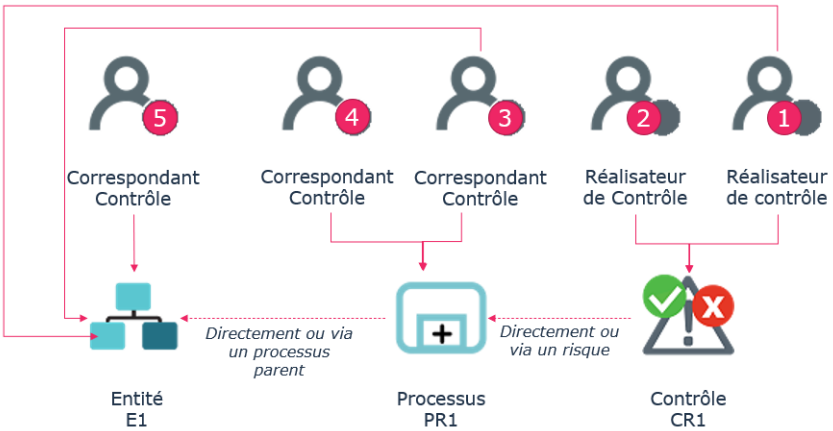
Logique de définition des répondants

Les répondants aux questionnaires de contrôle peuvent être définis sur :

- des entités
- des processus reliés aux entités (directement ou via le processus parent)
- des contrôles reliés aux processus (via un risque ou directement)

  ☛ *Voir aussi Contextualiser les contrôles.*

Ci-dessous l'ordre logique utilisé pour calculer les répondants sur les contrôles :



Le répondant du contrôle est calculé dans cet ordre :

1. un réalisateur du contrôle localisé sur une entité
2. un réalisateur du contrôle sans localisation
3. un correspondant de contrôle sur un processus avec localisation
4. un correspondant de contrôle sur un processus sans localisation
5. un correspondant de contrôle sur une entité

Spécifier les répondants

Pour spécifier les répondants, voir :

- Spécifier les réalisateurs du contrôle.
- Spécifier les responsabilités
- Spécifier les responsabilités au sein d'une entité

Évaluation des contrôles par entité et texte de référence

Le modèle d'évaluation "Évaluation des contrôles par entité et texte de référence" permet d'évaluer la conformité informatique de l'organisation aux réglementations applicables.

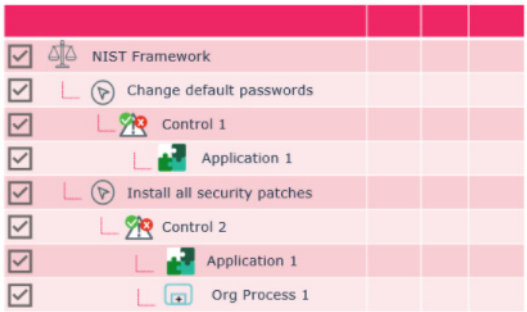
Contextes de l'évaluation

Les contrôles sont évalués dans le contexte de processus et applications.

L'évaluation porte sur les contrôles liés à une obligation appartenant à un texte de référence, et qui impacte :

- un processus relié directement ou indirectement à l'entité
- une application reliée à un processus, lui-même relié directement ou indirectement à l'entité

Les contrôles sont à sélectionner dans l'arborescence suivante : ***Texte de référence > Obligation > Contexte (application ou processus) > Contrôle.***



☛ *Les contrôles peuvent être reliés à des risques, eux-même reliés aux applications ou processus.*

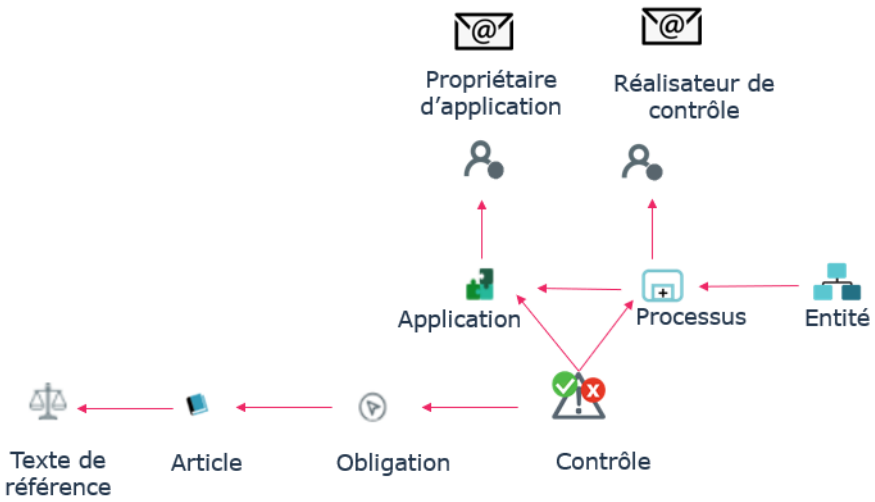
☛ *Sont exclus les contrôles reliés à une application non reliée à un processus.*

Pré-requis

Assurez-vous d'avoir :

- relié les contrôles à des obligations
- relié les contrôles à des processus ou à des applications.
- défini des répondants
  - pour les applications : le propriétaire d'application
  - pour processus : le réalisateur de contrôle

    ☛ *Voir Spécifier les responsabilités.*
- spécifié un e-mail pour chaque répondant



Utilisation possible

Ce modèle d'évaluation peut être utilisé dans le cadre :

- des campagnes d'évaluation de contrôles
- de l'évaluation directe multiple

> ☛ *Des rapports spécifiques permettent de suivre la démarche de mise en conformité informatique. Voir Rapports de conformité informatique et réglementaire.*

ÉVALUATION DIRECTE DES CONTRÔLES

Hopex GRC permet d'évaluer les contrôles en termes de conception et d'efficacité.

Vous pouvez évaluer les contrôles :

- directement,
- par l'intermédiaire de questionnaires envoyés à une population identifiée.

> ☛ *Pour l'évaluation par questionnaire, voir Campagnes d'évaluation.*
>
> ☛ *Voir aussi : Pré-requis à l'évaluation des contrôles.*

Contexte de l'évaluation directe

Dans le cadre de l'évaluation directe, les valeurs des caractéristiques des contrôles peuvent être spécifiées de deux façons :

- dans les propriétés de chaque contrôle : Évaluer un contrôle.
- globalement : Évaluer plusieurs contrôles simultanément

Il s'agit d'une évaluation à dire d'expert.

> ☛ *Vous pouvez évaluer les contrôles pour lesquels vous avez des droits en édition.*

L'évaluation directe est effectuée pour tous les objets contextes disponibles dans la section **Périmètre** des caractéristiques du contrôle :

> ☛ *Pour plus de détails sur la contextualisation des contrôles, voir également Contextualiser les contrôles.*

Évaluer un contrôle

> ☛ *Avant d'évaluer un contrôle, vous devez vous assurer qu'il a été correctement contextualisé. Pour plus de détails, voir Contextualiser les contrôles.*

Pour évaluer directement un contrôle :

1. Ouvrez la fenêtre de propriétés d'un contrôle.
2. Sélectionnez la page **Évaluation** puis cliquez sur **Nouvelle évaluation**.

> ☛ *Si le contrôle n'a pas été correctement contextualisé, un avertissement apparaît (un contrôle doit être relié à un processus, qui lui doit être relié à une entité).*

3. Dans l'assistant qui apparaît, sélectionnez le(s) contexte(s) à inclure dans l'évaluation du contrôle.

4. Cliquez sur **Suivant**.
   Vous pouvez sélectionner les valeurs qui caractérisent ce contrôle (contextualisé) en termes de :
   - conception
   - efficacité

   ☛ *D'autres questions peuvent être posées si votre administrateur a paramétré le questionnaire fourni en standard.*
5. Dans les champs **Conception** et **Efficacité**, indiquez si le contrôle est :
   - satisfaisant
   - insatisfaisant

   ☛ *Les valeurs sont appliquées à l'ensemble des nœuds d'évaluation sélectionnés préalablement.*
6. Dans le calendrier, spécifiez la date de la mesure.
   Par défaut il s'agit de la date du jour. Vous pouvez sélectionner une date antérieure à la date du jour.
7. Cliquez sur **OK**.
   Des mesures de contrôle sont créées pour chaque nœud d'évaluation (c'est-à-dire le contrôle dans un contexte particulier).

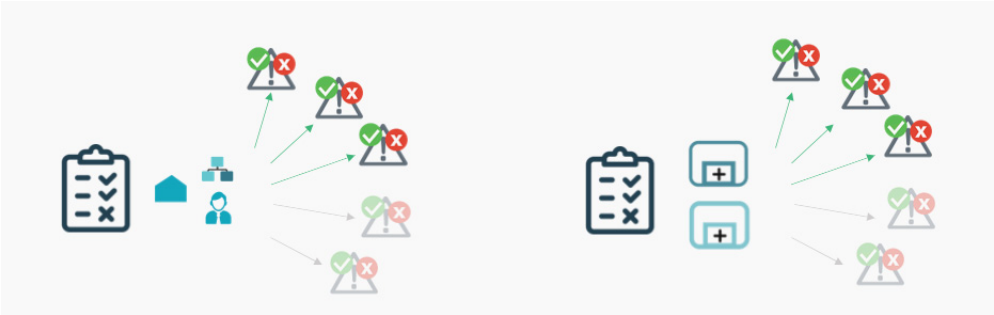
Vous pouvez créer de la même façon d'autres mesures à des dates différentes.

Évaluer plusieurs contrôles simultanément

Si vous devez évaluer plusieurs contrôles, il peut être plus rapide d'utiliser l'évaluation multiple. En effet, cette fonctionnalité vous permet d'affecter une même valeur à plusieurs nœuds d'évaluation de contrôles différents.

☛ *Un nœud d'évaluation est constitué de :*

- *un objet à évaluer*
- *éventuellement, un ou plusieurs objets contextes (entités, processus ou opérations)*



Pour évaluer plusieurs contrôles simultanément :

1. Dans la barre de navigation cliquez sur **Évaluation > Évaluation directe > Évaluation multiple des contrôles**.
2. Cliquez sur **Nouvelle évaluation**.

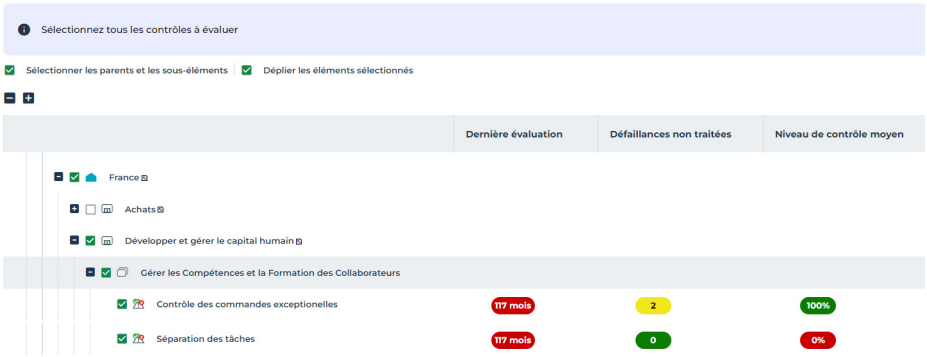
3. Dans la fenêtre qui apparaît, sélectionnez le modèle d'évaluation désiré :
   - "Évaluation des contrôles"
   - "Évaluation des contrôles par entité et texte de référence"

   ☛ *Pour plus de détails, voir Modèles d'évaluation pour les contrôles.*

4. Sélectionnez les objets de contexte qui vous intéressent.

   ☛ *Si vous avez sélectionné le modèle "Évaluation des contrôles", une arborescence vous est proposée. Un contrôle est évalué dans le contexte des éléments de la branche qui remonte du contrôle jusqu'à la racine.*

   Des informations en colonnes sont disponibles pour vous permettre de sélectionner les contrôles à évaluer.



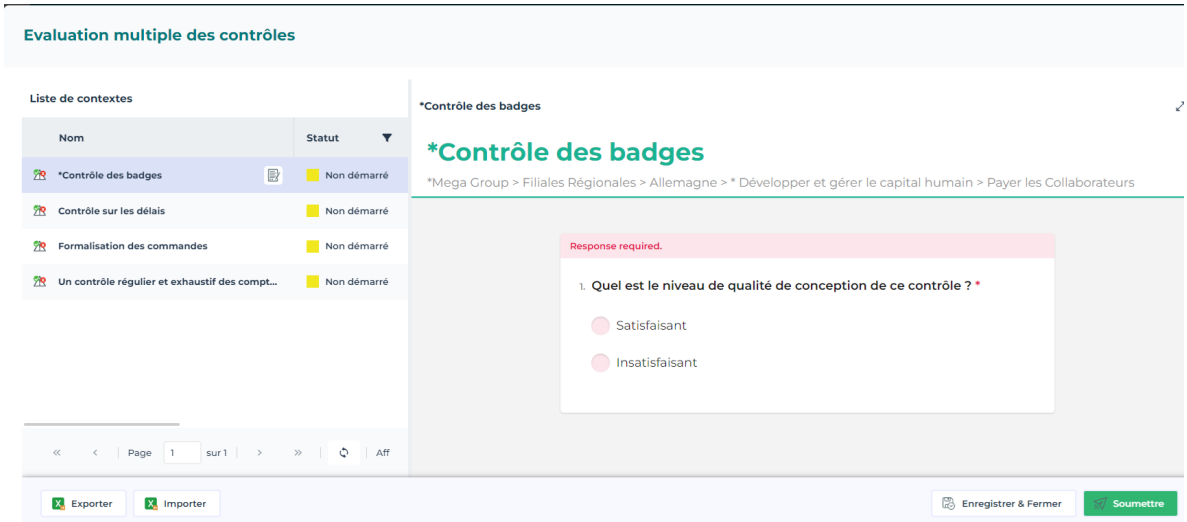
Dans l'exemple ci-dessus, si vous avez sélectionné le Processus "Gérer les compétences...", tous les contrôles et objets contextes se situant à un niveau inférieur sont sélectionnés, ainsi que tous les objets contextes parents jusqu'à la racine de l'arborescence.

☛ *Si vous dé-sélectionnez un nœud d'une branche, seuls les enfants de cette branche sont dé-sélectionnés.*

5. Cliquez sur **Suivant**.
   Un récapitulatif de l'évaluation apparaît, vous permettant ainsi d'avoir une vue d'ensemble des objets que vous allez évaluer.

6. Cliquez sur **OK**.
   La liste des contrôles à évaluer dans un contexte particulier apparaît.

7. Indiquez le niveau de qualité de **Conception** du contrôle et son niveau d'**Efficacité** :
   - Satisfaisant
   - Insatisfaisant



8. Après avoir répondu aux questions, cliquez sur **OK**.

   ☛ *Vous pouvez également choisir de fermer simplement le questionnaire pour y revenir et reprendre l'évaluation plus tard.*

Des évaluations sont créées dans la page **Évaluation** de la fenêtre de propriétés des contrôles. Pour plus de détails, voir Afficher les résultats d'évaluation de contrôle.

RÉSULTATS D'ÉVALUATION DES CONTRÔLES

Afficher les résultats d'évaluation de contrôle

Pour afficher les résultats d'évaluation réalisées sur un contrôle :

- A partir du registre de contrôles, sélectionnez la page **Évaluation** des propriétés du contrôle concerné.

Le **Niveau de contrôle** est automatiquement calculé à partir des valeurs des caractéristiques spécifiées (satisfaisant/insatisfaisant).

Voir aussi : Mode de calcul des résultats des évaluations.

☛ *Seul l'administrateur fonctionnel GRC peut supprimer les résultats de l'évaluation (c'est-à-dire les nœuds d'évaluation).*

*Pour supprimer un nœud d'évaluation, sélectionnez-le et cliquez sur **Supprimer**.*

Analyser les résultats d'évaluation de contrôle

Rapports instantanés

Les rapports instantanés offrent une représentation graphique statistique des données. Vous pouvez générer des rapports instantanés sur une sélection d'évaluations afin de visualiser graphiquement certaines données ou comparer les évaluations sur des caractéristiques spécifiques.

Pour lancer un rapport instantané sur un ensemble d'évaluations d'un contrôle :

1. Affichez les propriétés du contrôle évalué et cliquez sur la page **Évaluation**.
2. Sélectionnez les évaluations en question.
3. Cliquez sur le bouton **Rapport instantané**.
4. Sélectionnez le type de rapport à créer puis, si nécessaire, les caractéristiques à analyser.

Rapports d'analyse dédiés

Outre les rapports instantanés, **Hopex GRC** offre des rapports types dédiés qui facilitent l'analyse des contrôles évalués.

Mode de calcul des résultats des évaluations

MetaAttribut	Calculé / Non calculé	Explications
Conception du contrôle (CI)	Calculé via la macro [Internal Control - Control Attributes]	- si ***noeud d'évaluation***, valeur calculée depuis la caractéristique évaluée "Conception de contrôle" (CI). - si ***noeud d'agrégation***, valeur calculée depuis la caractéristique évaluée "Pourcentage moyen de niveaux de contrôles acceptés".
Efficacité du contrôle (CI)	Calculé via la macro [Internal Control - Control Attributes]	- si **noeud d'évaluation**, valeur calculée depuis la caractéristique évaluée "Efficacité". - si ***noeud d'agrégation***, valeur calculée depuis la caractéristique évaluée "Pourcentage moyen de niveaux de contrôles acceptés".
Niveau de contrôle (CI)	Calculé via la macro [Internal Control - Computed Control Attributes]	Résultat arrondi issu de la formule : Conception du contrôle (CI) * Efficacité du contrôle (CI)

☛ *Pour plus de détails sur l'agrégation, voir Les schémas d'agrégation.*

EXÉCUTER LES CONTRÔLES

Des contrôles sont effectués périodiquement par les responsables de processus, pour vérifier que les processus opérationnels se sont bien déroulés et que leurs résultats sont conformes aux attentes.

Les contrôles sont exécutés dans leur contexte, par processus et entité. Ils sont présentés sous forme de check-lists. Ces check-lists sont des questionnaires présentant des questions sur chaque contrôle.

Le nombre de check-lists envoyées dépend de la taille de la population et de l'échantillon.

Des rapports générés automatiquement permettent de suivre l'état d'avancement de l'exécution des contrôles et de consolider les résultats.

- ✓ Préparer l'exécution des contrôles
- ✓ Modèle d'évaluation pour le contrôle permanent
- ✓ Créer une campagne d'exécution
- ✓ Fonctionnement d'une campagne d'exécution
- ✓ Remplir les check-lists d'exécution de contrôles
- ✓ Gérer les check-lists d'exécution
- ✓ Résultats des check-lists d'exécution
- ✓ Rapports concernant l'exécution des contrôles

PRÉPARER L'EXÉCUTION DES CONTRÔLES

Pour pouvoir lancer des campagnes d'exécution, vous devez avoir au préalable défini les conditions d'exécution des contrôles :

- questions (check-lists)
- calendriers de pilotage
- taille de la population et de l'échantillon
- répondants
- contextualisation des contrôles.

Définir des étapes de contrôles

Vous devez définir le contenu des check-lists utilisées lors de l'exécution des contrôles.

Ces questions à définir sur les contrôles sont appelées "étapes de contrôle".

Pour plus de détails sur les types de questions, voir Types de questions.

> ☛ *Seules les réponses de type "OK/KO" sont agrégées dans les résultats des campagnes d'exécution. Les autres types de réponses sont pris en compte à titre d'information seulement.*

Pour créer des questions sur un contrôle :

1. Dans la fenêtre de propriétés du contrôle, sélectionnez la page **Exécution**.
2. Dans la section **Étapes de contrôle**, cliquez sur le bouton **Créer**.

Un assistant d'édition s'ouvre, dans lequel vous pouvez créer vos étapes de contrôles sous forme de questions.

Pour plus de détails sur son utilisation, voir Définir les modèles de questionnaires.

Si des étapes de contrôles ont été définies au préalable comme modèle, l'assistant vous propose de :

- créer de nouvelles étapes de contrôle, ou
- initialiser les étapes de contrôle à partir d'un modèle existant.

> ☛ *Pour plus de détails, voir Créer des étapes de contrôles à partir d'un modèle existant.*

Rendre réutilisables les étapes de contrôles

Après avoir créé des étapes de contrôle, vous pouvez décider d'en faire un modèle pour pouvoir les réutiliser.

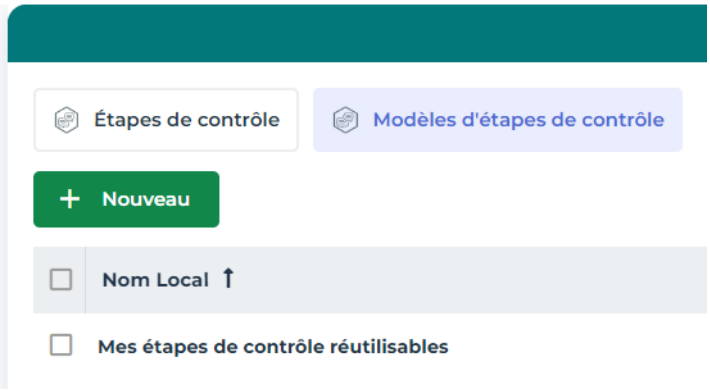
Pour pouvoir réutiliser des étapes de contrôle :

1. Définissez des étapes de contrôle.

> ☛ *Voir Définir des étapes de contrôles.*

2. Cliquez sur le bouton **Enregistrer comme modèle**.
3. Donnez un nom à vos étapes de contrôles réutilisables.

Une fois le "modèle" créé, vous pouvez le visualiser dans le menu **Évaluation > Étapes d'exécution de contrôles > Modèles d'étapes de contrôle**.



Dorénavant, lorsque vous créerez des étapes de contrôle, un assistant vous proposera d'en créer de nouvelles ou d'initialiser ces étapes de contrôle avec un modèle existant.

☛ *Si vous ne souhaitez plus proposer ces étapes de contrôles comme modèle, dans la page **Exécution** du contrôle concerné, cliquez sur le bouton **Ne plus proposer comme modèle**.*

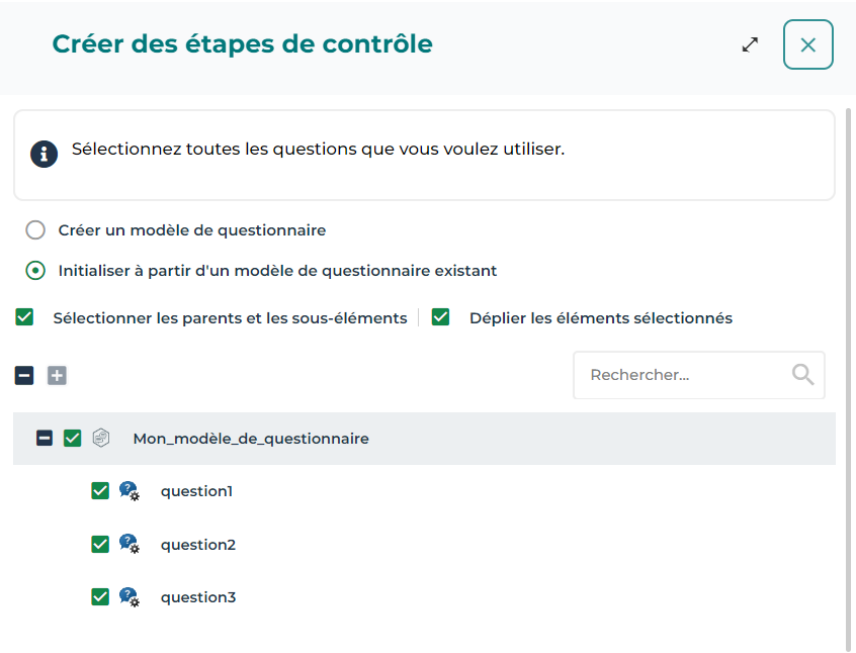
Créer des étapes de contrôles à partir d'un modèle existant

Pour créer des étapes de contrôles à partir d'un modèle existant :

1. Voir Définir des étapes de contrôles

2. Cliquez sur **Initialiser à partir d'un modèle existant**.

   ☛ *Sélectionnez le modèle de questionnaire ainsi que les questions à inclure (vous pouvez en sélectionner certaines seulement).*



   ☛ *Les modèles d'étapes de contrôle disponibles se trouvent dans **Évaluation > Étapes de contrôle d'exécution**.*

Définir le calendrier de pilotage des contrôles

Pour définir la périodicité d'exécution, vous devez spécifier le calendrier de pilotage à utiliser sur chaque contrôle.

☛ *Vous pouvez spécifier le calendrier d'exécution des contrôles uniquement après avoir créé un questionnaire (c'est-à-dire des étapes de contrôle).*

Pour créer un calendrier de pilotage, voir Gérer les calendriers de pilotage.

Spécifier un calendrier de pilotage sur le contrôle

Pour spécifier un calendrier de pilotage :

1. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Exécution**.
2. Assurez-vous qu'un questionnaire a bien été créé.
3. Sélectionnez une **Fréquence de l'exécution**.

   ☛ *Ce champ est à renseigner à titre informatif seulement.*

4. Sélectionnez un **Calendrier de pilotage**.
   Il existe des calendriers de pilotage pour différentes périodicité d'exécution :
   - quotidien
   - mensuel
   - hebdomadaire

Modifier un calendrier de pilotage après création d'une campagne

Si vous modifiez le calendrier de pilotage de contrôles inclus dans une campagne d'exécution en cours, vous devez re-planifier les check-lists.

Pour vous assurer que toutes les check-lists sont correctement planifiées :

1. Dans la fenêtre de propriétés d'une campagne d'exécution, sélectionnez la page **Sessions**.
2. Cliquez sur le bouton **Planifier les check-lists**.

   ☛ *Ceci concerne les contrôles qui utilisent un calendrier de pilotage non inclus initialement dans la campagne, ou les contrôles dont le calendrier de pilotage a été modifié.*

Définir la taille de la population totale et de l'échantillon

☛ *Cette étape est facultative.*

Vous pouvez définir :

- la **Taille de la population totale** : nombre total d'objets
- la **Taille de l'échantillon** : pourcentage de la population réellement contrôlée

  ☛ *Ces informations sont facultatives.*

  Par exemple :

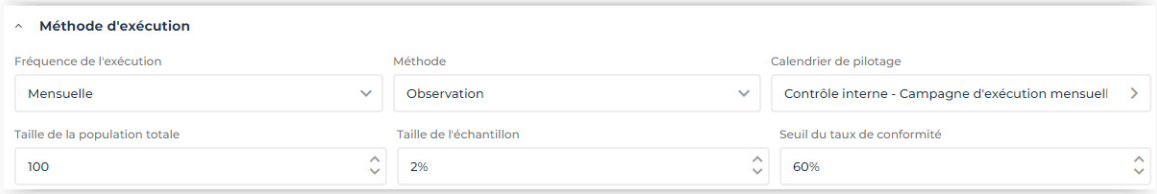
  - **Contrôle** : "Vérifier que les contrats sont signés"
  - **Population** : 20 (20 contrats)
  - **Taille de l'échantillon** : 10% (2 contrats seront vérifiés)

  Le propriétaire du contrôle reçoit une check-list avec deux lignes à remplir (une ligne par contrat)

Pour spécifier la population et la taille de l'échantillon :

1. Dans la fenêtre de propriétés du contrôle, sélectionnez la page **Exécution**.
2. Dépliez la section **Méthode d'exécution**.

3. Renseignez les données comme suit :



☛ *Le **Seuil de conformité** permet de calculer le résultat d'exécution. Le contrôle est jugé satisfaisant si le taux de conformité est supérieur ou égal au seuil de conformité.*

Définir les répondants

Les répondants des check-lists sont les personnes déclarées responsables des contrôles pour une entité donnée.

Vous devez définir les personnes chargées de remplir les check-lists d'exécution sur chaque contrôle.

La logique de définition des répondants est la même que pour l'évaluation des contrôles par entité. Voir Évaluation des contrôles par entité.

Relier les contrôles aux processus de l'entité

Les contrôles sont exécutés dans le cadre de processus organisationnels/métiers, reliés aux entités de l'organisation.

Pour relier les contrôles aux processus, voir Contextualiser les contrôles.

MODÈLE D'ÉVALUATION POUR LE CONTRÔLE PERMANENT

Les campagnes d'exécution sont des campagnes d'évaluation automatiques avec un modèle d'évaluation spécifique.

Le modèle d'évaluation "Exécution du contrôle permanent" est sélectionné par défaut à la création de la campagne d'exécution. Ce modèle d'évaluation :

- vous invite à renseigner une entité.
- permet d'identifier tous les contrôles utilisés par les processus rattachés à cette entité et à ses sous-entités.

Répondants

Les répondants des check-lists sont les personnes déclarées responsables des contrôles dans l'entité ou ses sous-entités.

Check-list envoyées

Une check-list est envoyée pour chaque couple Contrôle évalué/Répondant.

Si le répondant est responsable de plusieurs contrôles, celui-ci reçoit plusieurs questionnaires.

Le nombre de nœuds d'évaluation dans une check-list dépend de la taille de la population et de l'échantillon spécifiés dans les propriétés du contrôle.

☛ *Pour plus de détails, voir Définir la taille de la population totale et de l'échantillon.*

```
Par exemple :
Si taille de la population = 10 et si échantillon = 20%
Alors nombre de nœuds d'évaluation = 10*0,2 = 2
```

Calcul des réponses

Seules les réponses de type OK/KO sont prises en compte.

☛ *Pour plus de détails sur la définition des réponses d'un questionnaire, voir Types de questions.*

Résultats agrégés

Tous les nœuds ayant le même contrôle et même contexte sont agrégés. Les valeurs suivantes sont calculées :

- **Taux de conformité** : nombre de nœuds "OK" / nombre total de nœuds
- **Pourcentage d'achèvement** : pourcentage de questionnaires totalement remplis
- Le **Résultat d'exécution** est déclaré satisfaisant si le taux de conformité est supérieur ou égal au seuil de conformité.

☛ *Le seuil de conformité a été renseigné dans les propriétés du contrôle évalué.*

CRÉER UNE CAMPAGNE D'EXÉCUTION

Pour créer une campagne d'exécution :

1. Dans la barre de navigation, sélectionnez **Évaluation > Campagnes > Campagnes d'exécution**.
2. Cliquez sur **Nouveau**.

   ☛ *Le modèle d'évaluation "Exécution du contrôle permanent" est sélectionné par défaut. Pour plus de détails, voir Modèle d'évaluation pour le contrôle permanent.*

   Vous allez maintenant définir la façon de spécifier le périmètre de votre campagne.
3. Dans le champ **Définir le périmètre via une arborescence**, sélectionnez, au choix :
   - **Oui** : une arborescence permet de définir le périmètre de manière précise, mais ne permet pas de prendre en compte les éventuels contrôles ajoutés après création de la campagne.

     ☛ *Si vous choisissez cette option, voir Définir le périmètre via une arborescence.*
   - **Non** : un champ **Entité racine** vous est proposée.

     ☛ *A chaque échéance, le périmètre est recréé. Cela signifie que si de nouveaux contrôles ont été ajoutés, ils sont pris en compte lors de la prochaine session d'exécution planifiée.*
4. Modifiez éventuellement les dates proposées.

   ☛ *La **Date de début** de la campagne marque le démarrage de la campagne d'exécution.*
5. Cliquez sur **Suivant**.
   Un récapitulatif de la campagne d'exécution apparaît.

   ☛ *Voir Afficher le récapitulatif de la campagne d'exécution.*
6. Cliquez sur **OK**.
   La campagne apparaît dans la liste. Elle est démarrée automatiquement :
   - à la date de début spécifiée sur la campagne
   - à l'heure indiquée sur le calendrier de pilotage

     ☛ *Voir Consulter la planification d'une campagne d'exécution.*

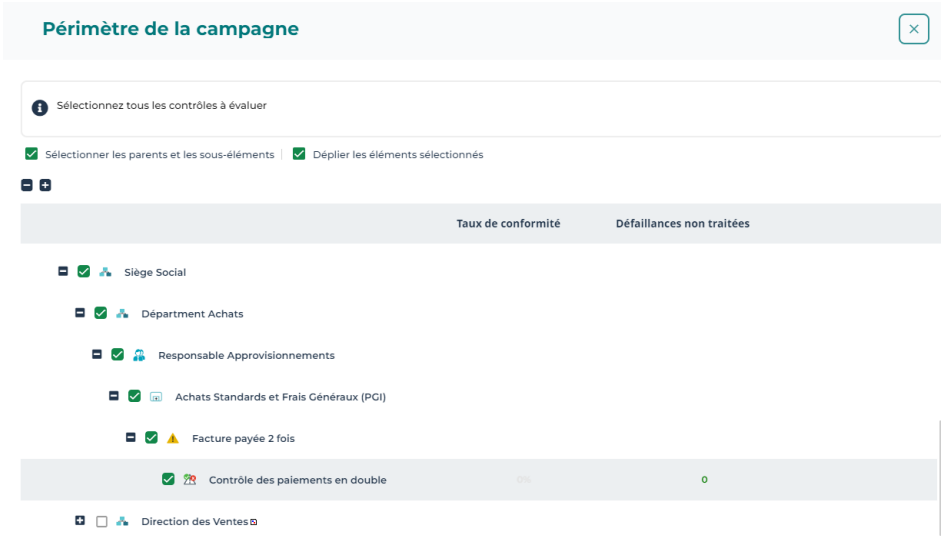
Définir le périmètre via une arborescence

Pour définir le périmètre de votre campagne :

1. Voir Créer une campagne d'exécution.
2. Affichez la page de l'assistant permettant de définir le périmètre.

3. Sélectionnez tous les contrôles à évaluer dans l'arborescence.
   Des colonnes vous guident dans le choix des contrôles à sélectionner :
   - **Taux de conformité**

     Le taux de conformité est le pourcentage de contrôles jugés satisfaisants.
   - **Défaillances non traitées** (en nombres)



Afficher le récapitulatif de la campagne d'exécution

Après avoir sélectionné le périmètre de la campagne (via une entité racine ou une arborescence), un récapitulatif de la campagne s'affiche. Il contient les élément suivants :

Informations générales (vue d'ensemble)

Nombre de :

- **erreurs** : les erreurs empêchent de lancer la campagne d'exécution :
  - le répondant n'est pas renseigné
  - le calendrier de pilotage n'est pas renseigné
- **avertissements**, par exemple :
  - la taille de la population ou de l'échantillon n'est pas renseignée
  - l'e-mail du répondant n'est pas renseigné
- objets évalués
- contextes d'évaluation
- répondants

Contextes

Les contextes apparaissent sous forme d'une hiérarchie de processus et entités :

Répondants

Les répondants sont les réalisateurs du contrôle.

☛ *Pour plus de détails sur la définition des responsabilités sur les contrôles, voir Responsabilités concernant les contrôles.*

☛ *Si aucun répondant n'est spécifié, faites un clic droit sur le contrôle et spécifiez-le dans la section **Responsabilités**.*

Objets évalués

Les contrôles évalués sont classés par fréquence d'exécution, avec en colonnes :

- le répondant
- les contextes : entités et processus organisationnels/métiers
- la taille de la population totale
- la taille de l'échantillon
- le taux de conformité
- le nombre de défaillances non traitées.

FONCTIONNEMENT D'UNE CAMPAGNE D'EXÉCUTION

Périodicité d'exécution des contrôles

Une campagne d'exécution regroupe plusieurs sessions d'exécution.

Chaque session d'exécution regroupe un ensemble de contrôles à exécuter à une même date.

Plusieurs sessions d'exécution sont créées en parallèle pour chaque type de calendrier de pilotage identifié.

Par exemple :

Une session est créée chaque semaine si un calendrier de pilotage hebdomadaire a été spécifié sur certains contrôles.

Une session est lancée chaque jour si un calendrier de pilotage quotidien a été spécifié sur d'autres contrôles.

Les contrôles sont regroupés dans chaque session en fonction du calendrier de pilotage qui leur a été relié. Voir Définir le calendrier de pilotage des contrôles.

Voir aussi : Exemples de lancement automatique de session.

Exemples de lancement automatique de session

Les sessions d'exécution sont lancées en fonction des informations suivantes :

- dates de début et de fin de la campagne d'exécution.
- dates de début/fin et récurrences spécifiées sur le calendrier de pilotage des contrôles

> ☛ *Pour plus de détails sur les calendriers de pilotage, voir Définir le calendrier de pilotage des contrôles.*

Lorsqu'une date d'échéance planifiée est atteinte, **Hopex** vérifie :

- que la campagne n'a pas été fermée manuellement
- que la date de fin de la campagne n'est pas dépassée

Si ces deux conditions sont vérifiées, la prochaine session est re-planifiée.

Exemple 1

Si la date de début spécifiée sur le calendrier de pilotage est postérieure à la date de fin de la campagne, les contrôles ne sont pas exécutés.

Exemple 2

Sur la date de pilotage, l'exécution est prévue tous les jours à 6h du matin.

La campagne est créée et la transition démarrée à 10h du matin.

Si la case **Exécuter à la date / heure de démarrage** n'est pas cochée, la campagne est lancée le lendemain matin à 6h.

> ☛ *Si la case est cochée, un message d'erreur indiquant que vous ne pouvez pas enregistrer une planification dans le passé apparaît.*

Exemple 3

La case **Exécuter à la date / heure de démarrage** est cochée.

Sur la campagne d'exécution, la date de première exécution planifiée est supérieure à la date d'aujourd'hui (date de début de la campagne).

Dans ce cas, c'est la date de début de la campagne qui marque le lancement de la session d'évaluation.

Consulter la planification d'une campagne d'exécution

Pour consulter les prochaines exécutions d'une campagne en cours :

1. Dans la barre de navigation, sélectionnez **Évaluation > Campagnes > Campagnes d'exécution.**
2. Ouvrez la fenêtre de propriétés de la campagne d'exécution et sélectionnez la page **Gantt**.
   La liste des échéances définies par le calendrier de pilotage apparaît.

Pour afficher les propriétés d'une session d'exécution dans le diagramme de Gantt :

- Faites un clic droit sur la session d'exécution et sélectionnez **Propriétés**.

La **Date de fin** indiquée sur la campagne définit la fin effective de la campagne. Pour plus de détails sur les sessions réellement lancées, voir Exemples de lancement automatique de session.

> ☛ *Les échéances indiquées correspondent à des jobs planifiés au niveau du "scheduler". A chaque exécution d'un job, une nouvelle session est créée. La session précédente est fermée.*

Définir des rappels

Le gestionnaire de campagnes d'exécution peut définir des rappels, qui consistent à envoyer un e-mail aux répondants après envoi et/ou avant fermeture de la check-list.

Modifier les rappels proposés en standard

Des rappels sont définis par défaut. Vous pouvez modifier les valeurs proposées.

Pour modifier les rappels proposées en standard :

1. Dans la barre de navigation, sélectionnez **Évaluation > Campagnes > Campagnes d'exécution.**
2. Ouvrez les propriétés d'une campagne d'exécution.
3. Dans la page **Caractéristiques**, dépliez la section **Rappels et dates de fermeture anticipée des check-lists**.

4. Définissez, pour chaque calendrier de pilotage, les éléments suivants :
   - Nombre de **Jours après soumission de la check-list**
   - Nombre de **Jours avant fermeture de la check-list**.

   ☛ *Tout changement dans la définition des rappels est pris en compte à la création de la prochaine session d'exécution.*

Désactiver les rappels

Pour désactiver les rappels :

❱ Videz les cellules du tableau de définition des rappels.

Fermer les check-lists de manière anticipée

Vous pouvez fermer de manière anticipée les check-lists de campagnes d'exécution liées à un calendrier de pilotage spécifique.

Cela permet de ne pas laisser les check-lists ouvertes trop longtemps si les campagnes sont lancées peu fréquemment.

Pour cela :

1. Dans la barre de navigation, sélectionnez **Évaluation > Campagnes > Campagnes d'exécution.**
2. Ouvrez les propriétés d'une campagne d'exécution.
3. Dans la page **Caractéristiques**, dépliez la section **Rappels et fermeture anticipée des check-lists**.
4. Dans la ligne correspondant au calendrier de pilotage concerné, spécifiez une valeur dans la colonne **Fermer après (en jours)**.

   Si vous indiquez 60 dans cette colonne, les check-lists sont fermées 60 jours après le démarrage de la session d'exécution.

REMPLIR LES CHECK-LISTS D'EXÉCUTION DE CONTRÔLES

Une fois la campagne d'exécution démarrée, vous pouvez remplir les check-lists. Pour cela vous pouvez vous connecter avec un utilisateur ayant le profil "Contributeur GRC".

☛ *Pour plus de détails, voir Gérer les questionnaires et check-lists.*

Accéder aux check-lists d'exécution

Pour accéder aux check-lists d'exécution :

1. Cliquez sur le lien de l'e-mail qui vous a été envoyé.

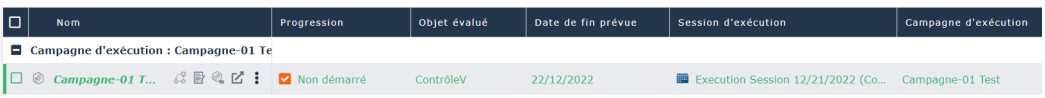
   ☛ *(alternative 1) Dans la page d'accueil du bureau "Contributeur GRC", cliquez sur **Mes tâches > Check-lists**.*

   ☛ *(alternative 2) Dans le bureau **Hopex GRC**, cliquez sur **Évaluation > Mes activités > Check-lists à remplir**.*

Remplir une check-list

Pour remplir les check-lists qui vous sont adressées :

1. Voir Accéder aux check-lists d'exécution.
2. Cliquez sur le nom de la check-list concernée.



3. Dans la liste qui apparaît, répondez aux questions de la check-list.

☛ *Si le contrôle a déjà été exécuté dans ce même contexte, les réponses apportées dans la dernière check-list sont affichées par défaut.*

4. Cliquez sur le bouton **Soumettre** puis **Terminer**.

   ☛ *Vous pouvez cliquer sur **Enregistrer & Fermer** si vous souhaitez soumettre vos réponses plus tard.*

Transférer une check-list

Si vous recevez un questionnaire par erreur, vous pouvez demander au responsable de la session de transférer le questionnaire à une autre personne.

Pour faire une demande de transfert :

1. Voir Accéder aux check-lists d'exécution.
2. Cliquez sur le nom de la check-list concernée.
3. Cliquez sur **Soumettre** puis sur **Demande de transfert**.
   Un responsable est notifié par e-mail et doit réassigner le questionnaire à une autre personne.

> ☛ *Les demandes de transfert sont exceptionnelles si le travail préparatoire à la création de la campagne d'exécution a été correctement réalisé.*

GÉRER LES CHECK-LISTS D'EXÉCUTION

Accéder aux check-lists

Vous pouvez visualiser les check-lists d'exécution des contrôles à tout moment.

Pour accéder aux check-lists :

- Dans le bureau **Hopex GRC**, Cliquez sur **Évaluation > Suivi**.
  Vous pouvez visualiser, à partir de la liste déroulante, les check-lists qui :
  - ont été envoyées dans le cadre de la campagne
  - ont déjà été remplies par les répondants
  - n'ont pas encore été remplies

Réassigner une check-list

Si une demande de transfert vous a été adressée, vous devez réassigner la check-liste à un autre utilisateur.

☛ *Pour plus de détails sur le transfert d'une check-list, voir Transférer une check-list.*

Pour réassigner une check-list :

1. Dans le bureau **Hopex GRC**, Cliquez sur **Évaluation > Mes activités > Check-lists à réassigner**.
2. Sélectionnez une check-list et ouvrez sa fenêtre de propriétés.

RÉSULTATS DES CHECK-LISTS D'EXÉCUTION

Pour afficher les résultats des check-lists d'exécution :

3. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Exécution**.
4. Dépliez la section **Résultats du contrôle permanent**.

Les nœuds d'évaluation (le contrôle exécuté dans chaque contexte) apparaissent sous forme de tableau.

Les résultats sont affichés en colonnes :

- **Pourcentage d'achèvement** : pourcentage de check-lists complètement remplies (sur le nombre total de check-lists)
- **Taux de conformité** : nombre d'objets jugés satisfaisants / nombre total d'objets

  ☛ *Seules les questions de type OK/KO/NA sont utilisées dans le calcul du taux de conformité.*
- **Résultat d'exécution** : le résultat d'exécution est jugé conforme si le taux de conformité est supérieur ou égal au seuil de conformité.

  ☛ *La **Taille de l'échantillon** et le **Seuil de conformité** sont rappelés à titre d'information. Les valeurs correspondantes ont été renseignées dans les propriétés du contrôle.*

RAPPORTS CONCERNANT L'EXÉCUTION DES CONTRÔLES

Des rapports vous permettent de suivre l'avancement et les résultats des check-lists.

Voir Rapports d'exécution des contrôles.

W

GÉRER LA CONFORMITÉ

Hopex GRC permet au directeur du contrôle interne chargé de la mise en conformité de :

- importer des données à partir du Common Controls Hub d'UCF ("Authority Documents", "Citations" et "Common Controls")

  ☛ *Pour utiliser l'assistant d'import, vous devez disposer du produit **HOPEX UCF**.*

- définir les réglementations auxquelles l'organisation doit se conformer ainsi que ses politiques internes
- définir le périmètre d'entités et processus sujets à cette mise en conformité
- procéder à des évaluations de la conformité informatique aux réglementations applicables

  ☛ *Un modèle d'évaluation spécifique est disponible. Voir Évaluation des contrôles par entité et texte de référence.*

- produire des rapports de conformité réglementaire et informatique

✓ A propos de "Unified Compliance Framework"
✓ Gérer l'environnement réglementaire
✓ Gérer le registre de conformité
✓ Rapports de conformité informatique et réglementaire

A PROPOS DE "UNIFIED COMPLIANCE FRAMEWORK"

UCF (Unified Compliance Framework) représente la plus grande bibliothèque de contenu réglementaire. UCF contient des :

- "Authority Documents"
- "Citations"
- "UCF Controls"

Le Common Controls Hub permet d'extraire facilement les données Unified Compliance Framework® dont vous avez besoin.

En utilisant les données UCF, le plan de mise en conformité est moins coûteux que si vous procédiez réglementation par réglementation.

Principaux concepts UCF

Authority Documents

Un "Authority Document" est un texte qui entre dans l'une des catégories suivantes:

- réglementations (textes de loi qui, en cas de non-respect, peuvent entraîner des sanctions),
- lignes directrices,
- standards / normes,
- bonnes pratiques.

> ☛ *Les "Authority Documents" sont convertis en textes de référence dans **Hopex**. Pour plus de détails, voir Visualiser les textes de référence.*

Citations

Les "Citations" sont des extraits de "Authority Documents". Elles sont associées à des "Common Controls".

> ☛ *Les "Citations" sont converties en articles ou sections dans **Hopex** (selon que la Citation est associée ou non à une obligation légale). Pour plus de détails, voir Visualiser les articles.*
>
> - *Toute Citation qui ne revêt pas de caractère légal mais qui contient d'autres Citations devient une section.*
> - *Toute Citation qui ne revêt pas de caractère légal et qui ne contient pas d'autres Citations devient un article (sans aucune pertinence pour l'organisation).*

UCF Controls

Les "Common Controls" sont des actions spécifiques qui doivent être effectuées pour se conformer à une obligation légale mentionnée dans une Citation.

> ☛ *Ils sont convertis en obligations dans **Hopex**. Pour plus de détails, voir Visualiser les obligations.*

En fonction de leurs liens avec les Citations, il est possible de distinguer plusieurs niveaux d'application de "Common Controls". Pour plus de détails, voir Liens entre concepts UCF.

Liens entre concepts UCF

Le niveau d'application est déterminé par l'association du Common Control à une Citation au sein d'un "Authority Document" et non pas par un attribut sur ce même Common Control.

Les Citations sont associés à des Common Controls, qui peuvent être :

- **mandated** (en **gras**)

  ☛ *Seuls les "Mandated Controls" sont obligatoires.*

  Les "Common Controls" sont obligatoires lorsqu'ils s'appliquent à au moins une Citation d'un "Authority Document".

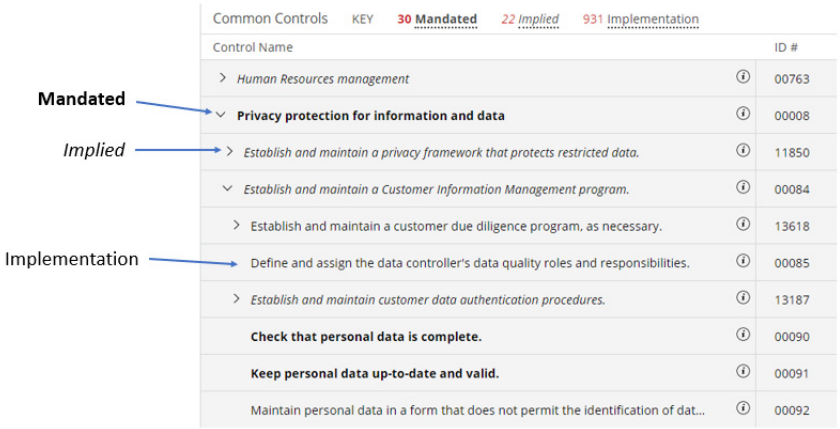
  Un "Common Control" qui est obligatoire a un impact sur les "Common Controls" auxquels ils contribuent et sur ceux qui l'impactent.

- *implied* (en *italique*)

  ☛ *Les "Implied Controls" sont des "Common Controls" qui ne sont pas obligatoires mais qui contiennent des "Mandated Controls" dans leur hiérarchie.*

- Implementation

  ☛ *Les "Common Controls" qui contribuent à d'autres "Common Controls" deviennent des "Implementation Controls". Ils fournissent des détails concernant la façon dont le "Mandated Control" doit être mis en œuvre.*



Créer une "Shared List"

Une "Shared List" (liste partagée) est une sélection de "Authority Documents" auxquels votre organisation doit se conformer et que vous avez choisis et sauvegardés dans votre espace Common Controls Hub.

Vous pouvez, par exemple, créer des listes concernant une région géographique de votre organisation, un sujet particulier ("Cybersécurité", "Banques et Finance").

Sélectionnez les "Authority Documents" auxquels vous devez vous conformer. Tous les Common Controls associés sont présentés dans une liste hiérarchique.

☛ *Une "Shared List" devient un ensemble de textes de référence une fois dans **Hopex** .*

Assurez-vous de n'inclure dans votre "Shared List" que les "Authority Documents" que vous voulez importer dans **Hopex**.

Correspondance entre concepts UCF et Hopex

UCF	Hopex	Icône dans HOPEX
Authority Document	Texte de référence	
Citation - Aucun "Mandated Control" associé - Contient d'autres Citations	Section	
Citation - Aucun "Mandated Control" associé	Article	
Citation - Aucun "Mandated Control" associé ET ne possède pas d'enfant	Article "feuille"	
UCF Common Control	Obligation	

GÉRER L'ENVIRONNEMENT RÉGLEMENTAIRE

Vous pouvez :

- importer du contenu UCF à partir d'une liste partagée (Shared List) créée en utilisant le Common Controls Hub
- visualiser les textes de référence et obligations dans **Hopex**
- définir les articles qui s'appliquent à l'organisation

> ☛ *Une fois que les données UCF ont été importées dans **Hopex**, il n'est pas possible de les exporter (pour les transférer vers un autre référentiel par exemple).*

Pour gérer votre environnement réglementaire dans **Hopex** :

❱ Dans la barre de navigation, sélectionnez **Conformité > Réglementations**.

Utiliser l'import UCF

Exigences préalables à l'import UCF

Les directeurs du contrôle interne ou les Managers GRC peuvent télécharger du contenu UCF ("Authority Documents", "Citations" et "Common Controls" et le mettre à jour.

Pour pouvoir importer ce contenu dans **HOPEX UCF**, vous devez avoir :

- **Hopex GRC** (ou **Hopex Internal Control** au minimum) ET **HOPEX UCF**
- un compte UCF et une clé API UCF
- une "Shared List" (liste partagée) avec les (seuls) "Authority Documents" que vous voulez importer.

  > ☛ *Pour plus de détails, voir Unified Compliance Framework.*

- paramétré les options UCF dans **HOPEX UCF**

  > ☛ *Dans le Common Controls Framework d'UCF, les informations sont généralement disponibles en anglais.*
  >
  > *Si vous souhaitez utiliser **HOPEX UCF** alors que vous utilisez **Hopex** dans une langue de données utilisateur autre que l'anglais, vous devez :*
  >
  > - *paramétrer la langue de données souhaitée (par exemple, le français, si vous souhaitez utiliser **Hopex** avec des données en français)*
  > - *procéder à l'import*
  > - *répéter l'opération (changer de langue de données + procéder à l'import) autant de fois que de langues souhaitées*

Paramétrer l'import UCF

Pour paramétrer l'import UCF :

1. Dans **Menu principal**, sélectionnez **Paramètres > Options**.
2. Dans la fenêtre d'options, dépliez **Outils > Echange de données > Import > Intégration UCF Common Controls Hub**.
3. Sélectionnez la case **Activer l'import UCF**.

4. Saisissez l'URL correspondant à l'API UCF.

   `https://api.unifiedcompliance.com/`

5. Saisissez votre **Clé d'authentification** pour l'API UCF.

   ☛ *Pour récupérer votre clé d'authentification dans votre espace de travail Unified Compliance Framework :*

   - *Cliquez sur Settings > API Manager > API Keys.*
   - *Cliquez sur "Create Credentials" et copiez-collez votre clé API.*

6. Cliquez sur **OK**.

Importer des données à partir du Common Controls Hub

Les responsables de la conformité doivent créer les éléments de l'environnement UCF dans Compliance **HOPEX UCF**. Il s'agit de :

- importer les données pertinentes à partir du Common Controls Hub d'UCF (Authority Documents, Citations et Controls)
- déclarer les articles appropriés comme étant pertinents pour votre organisation : voir Spécifier le contenu réglementaire applicable.

Pour importer les données UCF :

1. Dans la barre de navigation, sélectionnez **Conformité > Réglementations > Textes de référence**.
2. Cliquez sur **Importer du contenu UCF**.
3. Cliquez sur **Suivant.**
4. Sélectionnez la "Shared List" de votre Common Controls Hub.
5. Cliquez sur **Suivant**.
6. Sélectionnez le(s) "Authority Document(s)" que vous voulez importer dans **Hopex**.

   ☛ *Si vous mettez à jour un "Authority Document" déjà importé, il peut être utile de comparer les colonnes **Dernier import de mise à jour UCF** et **Dernière mise à jour UCF disponible**.*

7. Cliquez sur **Suivant**.

Spécifier le contenu réglementaire applicable

Pertinence du contenu réglementaire

Tous les articles/sections d'un texte de référence importé ne sont pas applicables à votre organisation.

Les responsables de la conformité doivent étudier les textes de référence importés, identifier le contenu applicable et le déclarer comme tel.

Seuls le contenu considéré applicable est visible des parties prenantes dans les registres **Hopex**.

☛ *Le contenu réglementaire que vous créez directement dans **Hopex** est automatiquement considéré comme étant applicable.*

Procéder à la revue des textes de référence après import

Une fois que les données UCF ont été importées, l'arborescence suivante apparaît (visible par les profils de type "Manager").

Cette arborescence affiche :

- les textes de référence (Authority Documents)
- les articles (Citations)
- les obligations légales rattachées (Common Controls).

Elle se base sur les relations entre obligations impactées / contributrices (supported/supporting) telles que définies dans UCF.

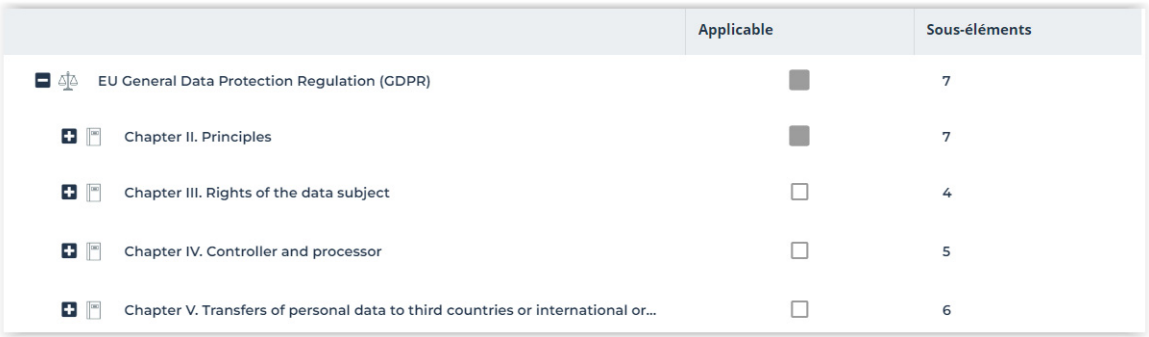
Vous pouvez, à partir de cette arborescence :

- procéder à la revue des textes de référence importés.
- spécifier le contenu applicable à votre organisation.

Sélectionner le contenu réglementaire pertinent pour votre organisation

Pour spécifier le contenu pertinent :

1. Dans la barre de navigation, sélectionnez **Conformité > Frameworks > Textes de référence**.
2. Dépliez l'arborescence et sélectionnez la case correspondant aux textes de référence / articles / sections auxquels vous devez vous conformer.



☛ *Le cadre grisé indique que seuls certains éléments du contenu ont été sélectionnés dans l'arborescence.*

Les données correspondant aux articles sélectionnés sont visibles par les contrôleurs internes dans le registre d'obligations. Voir Gérer le registre de conformité.

GÉRER LE REGISTRE DE CONFORMITÉ

Dans le registre de conformité, les contrôleurs internes peuvent gérer :

- les réglementations : textes de référence, articles, et obligations applicables à leur organisation.

  ☛ *Si vous avez des cadres réglementaires et exigences dans votre référentiel et que vous voulez les réutiliser dans **Hopex GRC**, voir Réutiliser les données réglementaires.*

  ☛ *Le registre de conformité n'affiche pas l'ensemble de ce qui a été importé d'UCF. Elle affiche uniquement les articles que le responsable de la conformité a estimé applicables après l'import. Pour plus de détails, voir Spécifier le contenu réglementaire applicable.*

- les règles internes à l'entreprise : les politiques d'entreprise

Concepts utilisés dans le registre de conformité

Concept HOPEX	Définition
Texte de référence	Un texte de référence est un texte qui entre dans l'une des catégories suivantes : réglementations (textes de lois qui peuvent entraîner des pénalités s'ils ne sont pas respectés), lignes directrices, standards et normes, bonnes pratiques.
Article (de texte de référence)	Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.
Section (de texte de référence)	Une section est une citation d'un texte de référence, qui n'est associée à aucune obligation légale et qui contient d'autres sections ou articles.
Obligation	Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.
Cadre de politique d'entreprise	Un cadre de politique d'entreprise constitue un ensemble de politiques d'entreprise. Les cadres de politique d'entreprise peuvent contenir des sections.
Politique d'entreprise	Une politique d'entreprise est un document interne émis par une organisation (code de bonne pratique, mesure de sécurité, etc.).

Accéder aux éléments du registre de conformité

Vous pouvez visualiser les éléments du registre de conformité via différentes listes et arborescences.

Afficher les éléments sous forme de listes

Vos obligations légales et politiques d'entreprise peuvent être classées dans différentes listes accessibles par un menu déroulant :

- sans contrôles
- reliées à des contrôles n'ayant jamais été exécutés
- reliées à des contrôles défaillants

Pour accéder à ces listes :

1. Dans la barre de navigation, sélectionnez **Conformité > Réglementations pertinentes** puis :
   - **Obligations**
   - **Politiques d'entreprise**

Des colonnes indiquent, pour chaque obligation :

- si l'obligation/la politique d'entreprise contraint votre organisation
- le nombre de contrôles de mise en œuvre

Pour lister les contrôles de mise en œuvre existants ou en créer :

1. Ouvrez la page de propriété de l'obligation/la politique d'entreprise et utilisez la section **Mise en œuvre**.

Afficher les obligations dans une arborescence de textes de référence

Pour afficher les obligations sous forme arborescente :

1. Dans la barre de navigation, sélectionnez **Conformité > Réglementations pertinentes > Obligations > Par texte de référence**.

Cette arborescence permet de visualiser les articles et obligations auxquels votre organisation doit se conformer. Elle fait apparaître :

- les textes de référence
- les obligations qui mettent en œuvre des articles
- les contrôles associés

Afficher les politiques d'entreprise sous forme arborescente

Pour afficher les politiques d'entreprise :

1. Dans la barre de navigation, sélectionnez **Conformité > Réglementations pertinentes > Politiques d'entreprise > Par cadre de politique d'entreprise**.

Cette arborescence permet de visualiser politiques d'entreprise auxquelles votre organisation doit se conformer.

Elle fait apparaître :

- le nombre de contrôles de mise en œuvre
- le taux de conformité

  📖 *Le taux de conformité est le pourcentage de contrôles jugés satisfaisants.*
- le niveau de contrôle

  📖 *Le niveau de contrôle permet de caractériser le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour atténuer le risque.*

Visualiser les textes de référence

Un texte de référence entre dans l'une des catégories suivantes :

- réglementations (textes de loi qui peuvent donner lieu à des sanctions en cas de non-respect)
- lignes directrices
- standards / normes
- bonnes pratiques

  ☛ *Les textes de référence correspondent aux "Authority Documents" provenant d'UCF.*

Accéder aux textes de référence

Une arborescence de textes de référence présente les articles pertinents.

Pour accéder à l'arborescence de textes de référence :

- Dans la barre de navigation, sélectionnez **Conformité > Frameworks > Textes de référence.**

L'arborescence présente des textes de référence et affiche :

- les obligations mettant en application les articles

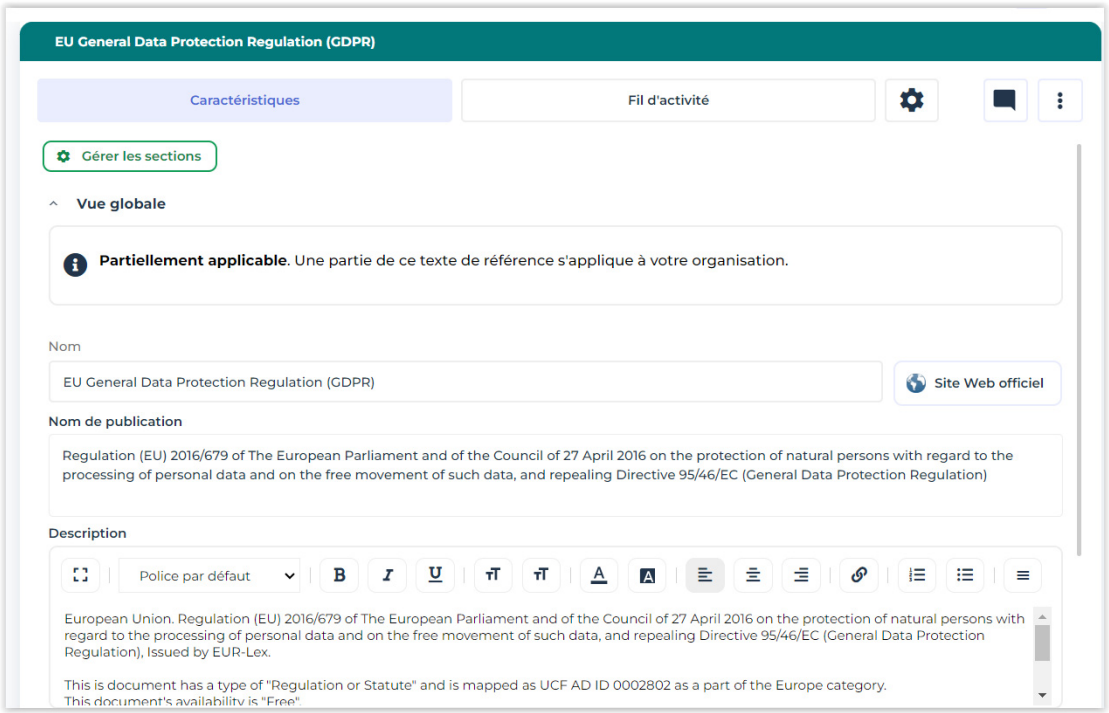
  ☛ *Pour plus de détails sur les obligations, voir Visualiser les obligations.*
- les contrôles **Hopex** de mise en oeuvre, le cas échéant.

  ☛ *Pour plus de détails sur les contrôles, voir Gérer les contrôles.*

Vue globale et description d'un texte de référence

La section **Vue globale** des caractéristiques d'un texte de référence permet d'afficher les caractéristiques générales (provenant du Common Controls Hub en cas d'import).

☛ *Ces caractéristiques ne peuvent pas être modifiées si le contenu provient d'UCF.*



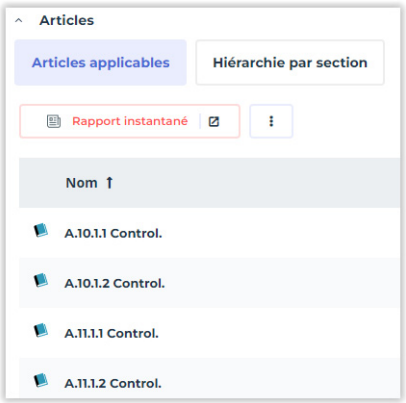
Contenu d'un texte de référence

Pour accéder au contenu réglementaire pertinent d'un texte de référence :

1. Dans la barre de navigation, sélectionnez **Conformité > Frameworks > Textes de référence.**
2. Sélectionnez le texte de référence approprié et ouvrez ses propriétés.
3. Dépliez la section **Articles**.

Vous pouvez accéder aux articles pertinents :

- via une liste d'**Articles applicables**
- via une **Hiérarchie par section**



Visualiser les articles

Un article est une citation d'un texte de référence qui est généralement associée à une obligation légale.

> ☛ *Les articles correspondent aux Citations importées d'UCF. Pour plus de détails, voir Principaux concepts UCF.*
>
> ☛ *Si la Citation d'origine contient une Citation mais n'est associée à aucun Common Control, elle devient une section dans **HOPEX UCF**.*
>
> *Si la Citation UCF ne contient pas de citation et n'est associée à aucun Common Control, elle devient un article "feuille" (non pertinent).*

La page de propriétés d'un article affiche :

- l'article ou la section parent
- les sous-articles, le cas échéant
- les éléments sujets à cet article (entités ou processus)
- les obligations légales associées

  > 🕮 *Une obligation est une interprétation de la loi qui contribue à la mise en application de tout article auquel votre organisation doit se conformer.*
- les contrôles de mise en oeuvre, le cas échéant

  > 🕮 *Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.*

Accéder aux articles

Pour accéder aux articles :

1. Dans la barre de navigation, sélectionnez **Conformité > Frameworks > Textes de référence** et dépliez l'arborescence.

Relier ou visualiser les objets sujets à un article

Il est possible d'associer des catégories de processus/processus ou des entités à des articles (ou sections). Cela permet de spécifier les parties de l'organisation sujettes à une mise en conformité.

Pour relier des catégories de processus / processus ou des entités à un article :

1. Dans la page de propriétés de l'article, dépliez la section **Éléments sujets** et reliez les objets comme approprié.

> ☛ *Une fois que les entités, processus ou catégories de processus sont reliés à l'article, un onglet **Articles** apparaît dans le périmètre de ces objets.*

Vous pouvez également visualiser les objets qui sont indirectement reliés à l'article.

> Exemple de lien indirect : Si un texte de référence a été relié à une entité, l'entité est indirectement liée à l'ensemble des sections et articles du texte de référence.

Mise en application d'un article

Pour en savoir plus sur la mise en application d'un article :

1. Ouvrez la page de propriétés de l'article et dépliez la section **Mise en application**.

Vous pouvez visualiser les:

- **Obligations** associées

> ☛ *Vous pouvez visualiser la qualification de l'obligation dans la colonne correspondante :*
>
> - *légale*
> - *connexe*
> - *préconisée*

- **Contrôles de mise en œuvre** associés

  Les contrôles de mise en œuvre apparaissant dans cette liste sont ceux reliés aux obligations de cette même section.

> ☛ *Les contrôleurs internes doivent concevoir des contrôles **Hopex** permettant de mettre en œuvre les obligations. Pour plus de détails sur les contrôles de mise en œuvre dans **Hopex**, voir Gérer les contrôles.*

Relier des documents métier

Vous pouvez relier des documents métier à article (ou à une section).

Visualiser les obligations

Les obligations constituent une interprétation de la loi et contribuent à la mise en application de tout article auquel votre organisation doit se conformer.

> ☛ *Les obligations correspondent aux Common Controls importés d'UCF. Pour plus de détails, voir Principaux concepts UCF.*

Accéder aux obligations

Pour accéder aux obligations contenues dans votre registre :

- Dans l'arbre de navigation, sélectionnez **Conformité > Réglementations pertinentes > Obligations > Obligations**.

  ☛ *Les obligations connexes de premier niveau apparaissent dans cette liste seulement si l'un de ses enfants revêt un caractère légal.*

Des colonnes vous indiquent :

- si l'obligation sélectionnée contraint l'organisation
- le nombre de contrôles de mis en œuvre associés

A partir de la liste déroulante vous pouvez visualiser les obligations classées en fonction de différents critères :

- **Obligations sans contrôles**

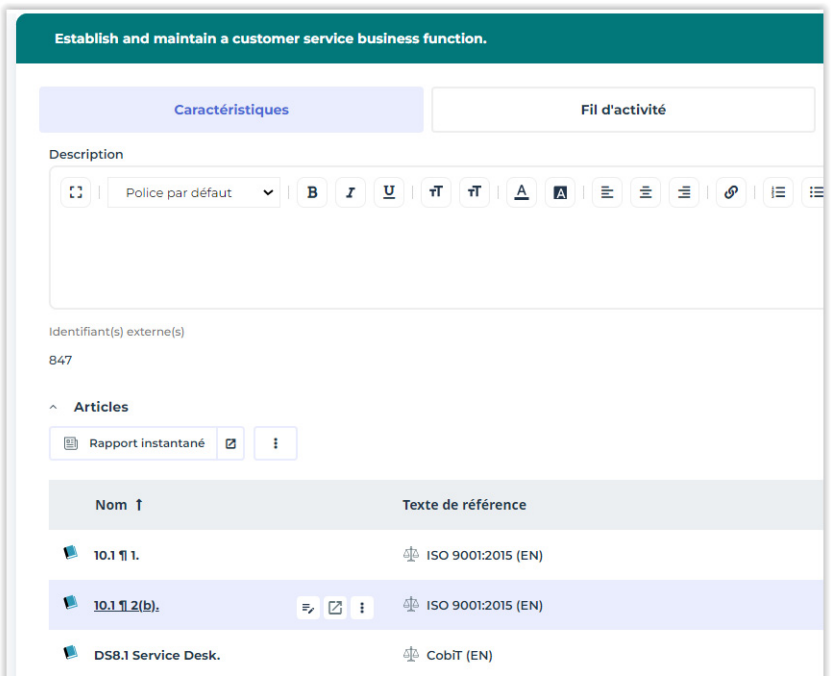
  ☛ *Pour créer un contrôle sur une obligation, dépliez la section **Mise en œuvre**.*

- **Obligations avec contrôles jamais exécutés**
- **Obligations avec contrôles défaillants**

Visualiser les articles associés à l'obligation

Une obligation légale est associée à un article.

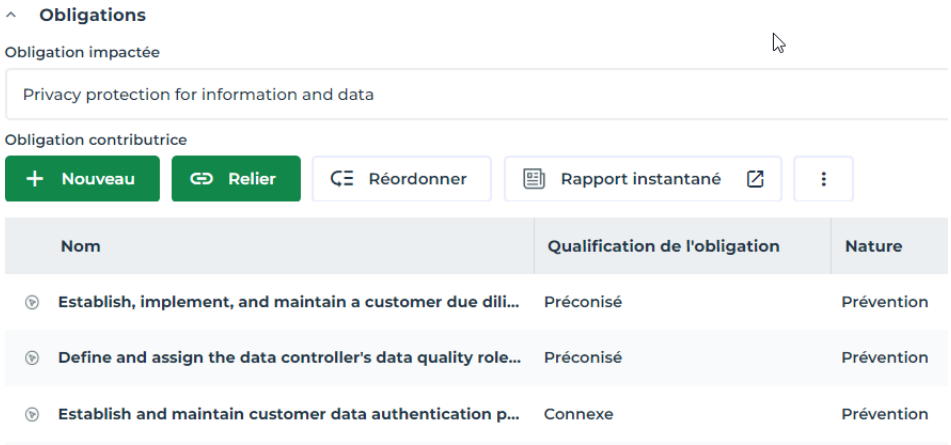
☛ *Il est utile d'avoir plusieurs articles dans la section **Articles** d'une obligation. Cela signifie que les obligations permettent de mettre en application plusieurs articles.*



Obligations impactées et contributrices

Les propriétés de l'obligation permettent de visualiser les inter-relations entre obligations :

- Obligation impactée
- Obligations contributrices



Mise en application des obligations

il existe trois niveaux de mise en application pour chaque obligation :

- ***légal***

  Toute obligation légale est associée directement à un article. Elle permet de mettre en œuvre un texte de référence.

- ***connexe***

  Une obligation connexe est une obligation qui ne revêt pas de caractère légal et qui est parent d'une obligation légale. Elle permet d'indiquer que l'une des obligations présente dans sa hiérarchie revêt un caractère légal.

- ***préconisé***

  Une obligation préconisée est une obligation qui ne revêt pas de caractère légal et qui est enfant d'une obligation légale. Elle donne des

détails concernant la façon de mettre en œuvre l'obligation légale et facilite sa mise en œuvre.

Niveau d'application des obligations	
Obligation connexe	- N'a pas de caractère légal - Contient au moins une obligation légale dans sa hiérarchie - Permet d'afficher les obligations légales présentes dans la hiérarchie UCF - Est impactée par une obligation légale
Obligation préconisée	- N'a pas de caractère légal - Apparaît sous une obligation légale (contribue à une obligation légale)
Obligation légale	- Contribue à une obligation connexe - Peut être impactée par des obligations préconisées - Peut contribuer ou être impactée par d'autres obligations légales

Visualiser les contrôles Hopex de mise en oeuvre des obligations

Les colonnes dans la liste des obligations donnent un aperçu des contrôles **Hopex** qui mettent en œuvre chaque obligation.

Pour avoir une vue détaillée des contrôles sur une obligation donnée :

1. Dans la barre de navigation, sélectionnez **Conformité > Réglementations pertinentes > Obligations**.
2. Ouvrez les propriétés d'une obligation.
3. Dépliez la section **Mise en œuvre**.

☛ *Vous pouvez également créer des contrôles à partir de cette section.*

Des informations vous sont fournies sur le contrôle ainsi que sur ses résultats d'exécution :

- **Nature du contrôle**

  ☛ *Voir Nature de contrôle.*

- **Niveau de contrôle**

  🕮 *Le niveau de contrôle permet de caractériser le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour atténuer le risque.*

  ☛ *Voir Niveau de contrôle.*

- **Dernier taux de conformité**
- **Dernier résultat d'exécution**

  ☛ *Pour plus de détails sur l'exécution des contrôles, voir Exécuter les contrôles.*

Relier des documents métier ou références externes

Vous pouvez relier des documents métier à une obligation ou créer une référence externe de type URL.

RAPPORTS DE CONFORMITÉ INFORMATIQUE ET RÉGLEMENTAIRE

☛ *Pour plus de détails sur les rapports, voir :*

- *Accéder aux rapports*
- *Créer un rapport*

Hopex GRC fournit des rapports permettant de suivre le processus de mise en conformité informatique et réglementaire.

Des rapports permettent de :

- visualiser le niveau de conformité d'une entité à la réglementation.
  ☛ *Voir Conformité réglementaire par entité.*
- distinguer, pour chaque texte de référence, les obligations qui sont mises en œuvre par des contrôles de celles qui ne le sont pas
  ☛ *Voir Mise en œuvre des obligations par texte de référence.*
- visualiser le niveau de conformité pour chaque texte de référence
  ☛ *Voir Conformité par texte de référence.*
- suivre l'évolution du processus de mise en conformité
  ☛ *Voir Vue générale de la conformité réglementaire.*
  ☛ *Voir Avancement de la mise en conformité réglementaire.*
- visualiser les défaillances qui impactent un type de contrôle donné (un type de contrôle qui se rapporte à la conformité informatique, par exemple).
  ☛ *Voir Défaillances par impact.*

Conformité réglementaire par entité

Le rapport "Conformité réglementaire par entité" présente le niveau de conformité agrégé d'une entité donnée aux textes de référence applicables.

Ce rapport affiche une arborescence de tous les processus et applications de l'entité pour lesquels un contrôle relié à des réglementations a été évalué.

Chemin d'accès

Barre de navigation > Rapports

Paramètres et lancement

Pour lancer le rapport de conformité réglementaire par entité :

1. Renseignez ses paramètres.

Paramètres	Remarques
Entité	Obligatoire Entité dont le niveau de conformité est à calculer.
Date de début et de fin	Facultatif Permet de définir l'intervalle de temps à prendre en compte pour agréger les résultats des évaluations. Si aucune date n'est spécifiée, toutes les données d'évaluation sont prises en compte dans le calcul du niveau de conformité.

2. Cliquez sur le bouton **Lancer l'agrégation**.

3. Cliquez sur **OK**.

Exemple

Les résultats pour chaque objet présent dans ce rapport sont calculés comme suit :

Type d'objet	**Calcul**
Application /Processus (dans le périmètre d'un contrôle)	Dernière évaluation du contrôle dans le contexte de l'application ou du processus. Résultats possibles : - Satisfaisant - Non satisfaisant - Non évalué
Contrôle (mettant en œuvre une obligation)	Pourcentage de contrôles satisfaisants (pour les applications ou processus contextes) A noter : ici, Non évalué = Non satisfaisant
Obligation (d'un texte de référence)	Moyenne des niveaux de contrôle pour les contrôles reliés à l'obligation.
Texte de référence (ayant dans son périmètre l'entité racine de l'arborescence)	Moyenne des niveaux de contrôle pour les obligations reliées au texte de référence.
Entité	Moyenne des niveaux de contrôles pour les textes de référence reliés à l'entité.

Mise en œuvre des obligations par texte de référence

Ce rapport permet au responsable de la conformité de s'assurer que les obligations sont effectivement mises en œuvre par des contrôles.

Il s'agit d'un diagramme à barres empilées qui présente la couverture globale d'une liste de textes de référence. Un texte de référence est considéré comme mise en oeuvre si toutes les obligations légales qu'il contient sont associées à un contrôle.

Chemin d'accès

Barre de navigation > Rapports

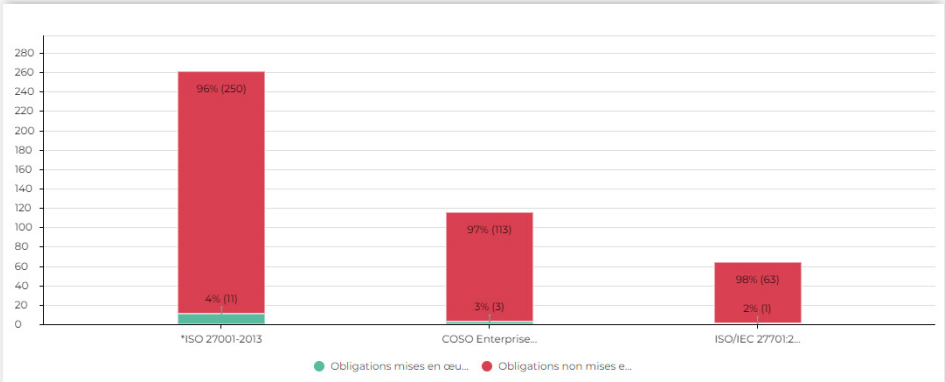
Paramètres

Paramètres	Remarques
Liste de textes de référence	Par défaut, le rapport s'applique à l'ensemble des textes de référence.

Résultats

Le rapport affiche, pour chaque texte de référence, le pourcentage :

- d'obligations reliées à au moins un contrôle (**obligations mises en oeuvre**)
- d'obligations qui ne sont reliées à aucun contrôle (**obligations non mises en oeuvre**).



Conformité par texte de référence

☛ *Ce rapport est également disponible sous forme de widget à ajouter dans votre tableau de bord. Pour l'ajouter, Dans la barre de navigation, cliquez sur* ***Tableau de bord*** *puis sur* ***Ajouter un widget > GRC > Conformité****.*

Ce rapport est un diagramme à barres empilées qui présente le niveau de conformité globale à une liste de textes de référence.

Chemin d'accès

Barre de navigation > Rapports

Paramètres

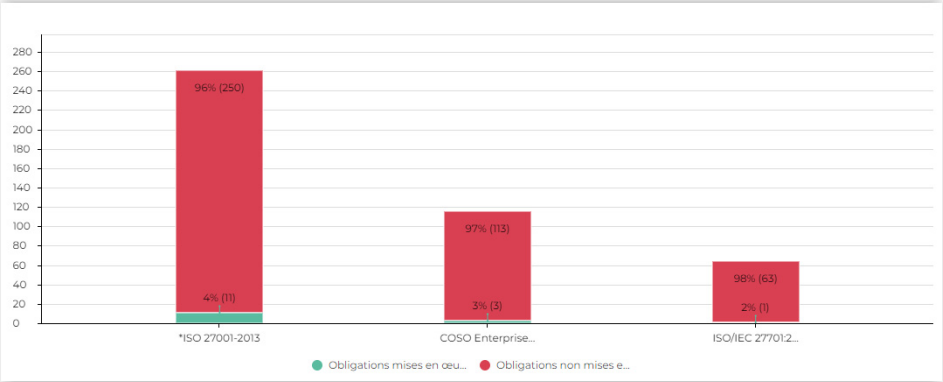
Paramètres	Remarques
Liste de textes de référence	Par défaut, le rapport s'applique à l'ensemble des textes de référence.

Résultats

Les résultats sont présentés sous forme d'histogrammes.

Chaque barre affiche le pourcentage de contrôles associés aux obligations légales et les regroupe par niveau d'évaluation :

- **Satisfaisant** : contrôles dont le Niveau de contrôle = 100% (ayant passé l'évaluation avec succès)
- **Insatisfaisant** : contrôles dont le Niveau de contrôle < 100% (n'ayant pas obtenu un score satisfaisant)
- **Non évalué** : contrôles avec niveau de contrôle non renseigné



Vue générale de la conformité réglementaire

Le rapport "Vue générale de la conformité réglementaire" permet de suivre le détail de la conformité à un texte de référence.

Chemin d’accès

Barre de menu > Rapports

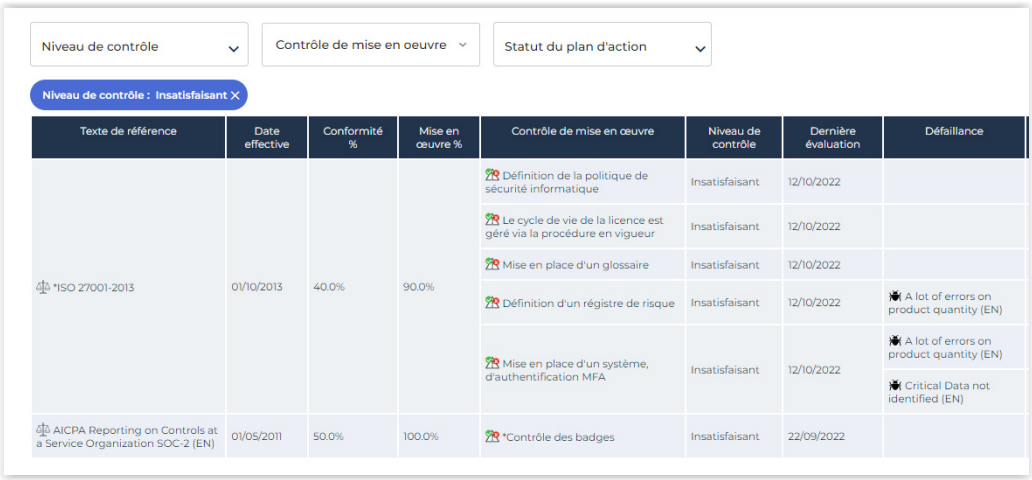
Paramètres

Paramètres	Remarques
Liste de textes de référence	Par défaut, le rapport s’applique à l’ensemble des textes de référence.

Résultats

A partir de ce rapport, vous pouvez surveiller, pour chaque texte de référence :

- le ***% de conformité*** : pourcentage de contrôles satisfaisants sur le nombre de contrôles reliés aux obligations du texte de référence.
- le ***% de mise en œuvre*** : pourcentage de contrôles évalués sur le nombre de contrôles reliés aux obligations du texte de référence.
- les évaluations de contrôles
  - ***Niveau de contrôle***
  - ***Dernière évaluation de contrôle***
- les défaillances et les plans d'action mis en œuvre :
  - ***défaillance***
  - ***% d'achèvement du plan d'action***
  - ***statut du plan d'action*** (dans les temps, en retard)
  - ***coût du plan d'action*** (estimation du coût du plan d'action)



Texte de référence	Date effective	Conformité %	Mise en œuvre %	Contrôle de mise en œuvre	Niveau de contrôle	Dernière évaluation	Défaillance
*ISO 27001-2013	01/10/2013	40.0%	90.0%	Définition de la politique de sécurité informatique	Insatisfaisant	12/10/2022	
				Le cycle de vie de la licence est géré via la procédure en vigueur	Insatisfaisant	12/10/2022	
				Mise en place d'un glossaire	Insatisfaisant	12/10/2022	
				Définition d'un registre de risque	Insatisfaisant	12/10/2022	A lot of errors on product quantity (EN)
				Mise en place d'un système, d'authentification MFA	Insatisfaisant	12/10/2022	A lot of errors on product quantity (EN)
							Critical Data not identified (EN)
AICPA Reporting on Controls at a Service Organization SOC-2 (EN)	01/05/2011	50.0%	100.0%	*Contrôle des badges	Insatisfaisant	22/09/2022	

Avancement de la mise en conformité réglementaire

Ce rapport est un graphique en radar qui représente l'évolution dans le temps du niveau de conformité d'une entité à un ensemble de réglementations.

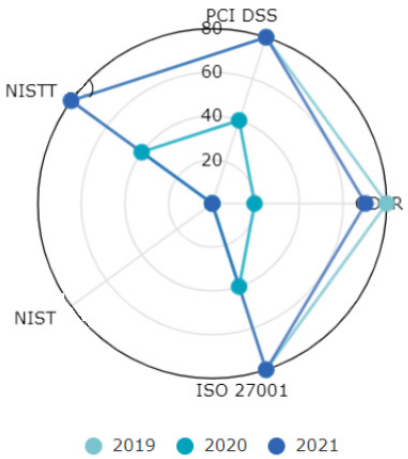
Chemin d'accès

Barre de menu > Rapports

Paramètres

Paramètres	Remarques
Entité	Organisation dont le niveau de conformité est à calculer
Textes de référence	Réglementations à inclure dans le graphique
Calendriers	Intervalles de temps pris en compte pour suivre l'évolution du niveau de conformité dans le temps

Exemple de rapport



TESTER LES CONTRÔLES

En complément des revues par la hiérarchie opérationnelle, des tests de contrôles peuvent être effectués. Ces tests consistent à mener une mission d'audit interne sur les contrôles. **Hopex GRC** permet aux contrôleurs internes :

- ✓ d'exécuter des missions de test sur site en remplissant des fiches de test
- ✓ d'évaluer ces missions de test exécutées
- ✓ d'évaluer les contrôles en termes de conception et d'efficacité via des questionnaires
- ✓ de mettre en oeuvre des plans d'action dans le but d'améliorer les contrôles pour lesquels des défaillances ont été mises en évidence.
- ✓ de remplir des notes de frais et des feuilles de temps

Le processus de test se déroule en trois phases.

- ✓ Préparer le test des contrôles
- ✓ Préparer les missions de test
- ✓ Exécuter les missions de test
- ✓ Suivre les missions de test

PRÉPARER LE TEST DES CONTRÔLES

☛ *Voir aussi Contextualiser les contrôles.*

☛ *Voir aussi : Administration fonctionnelle GRC.*

Définir les questions des fiches de test

Vous devez définir des questions (étapes de test) sur les contrôles pour pouvoir générer des fiches de test à usage des contrôleurs internes.

Pour créer les étapes de test d'un contrôle :

1. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Testing**.
2. Sous la section **Etapes de test**, cliquez sur le bouton **Créer un questionnaire**.
3. Dans la fenêtre qui apparaît, glissez-déplacez une question de type "OK/KO".
4. Cliquez sur **Enregistrer et Fermer**.

Définir la méthode de test

☛ *Pour pouvoir définir la méthode de test, vous devez avoir créé au préalable des questions (étapes de test) sur les contrôles.*

Pour renseigner les caractéristiques utiles au test des contrôles :

1. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Testing**.
   La section **Méthode de test** présente des caractéristiques concernant le testing.
2. Renseignez la **Fréquence** :
   - Annuelle
   - Trimestrielle
   - Semestrielle
3. Renseignez la **Méthode de test** :
   - Enquête
   - Inspection
   - Observation
   - Ré-exécution
4. Renseignez la taille de la **Population de test** : nombre total d'objets susceptibles d'être contrôlés (par exemple : 1000 factures ou 100 contrats).

5. Renseignez la **Taille de l'échantillon de test** : valeur dont les fiches de test vont hériter par défaut.

   ☛ *Pour plus de détails, voir Spécifier ou modifier la taille de l'échantillon.*

PRÉPARER LES MISSIONS DE TEST

Les fonctionnalités décrites ici concernent essentiellement le Manager GRC.

Le chef de mission intervient pour définir le programme de travail qui va permettre :

- d'exécuter les activités de test
- d'évaluer les contrôles via des questionnaires

La préparation des missions de test consiste à créer un plan de test, des missions de test, et à les planifier avant que les contrôleurs n'interviennent sur le terrain.

Créer un plan de test

La préparation du plan est effectuée par le directeur du contrôle interne.

Le plan est généralement défini sur une période d'une année. Ce plan contient toutes les missions de test à réaliser dans l'année.

> 🕮 *Le plan de test est la description du champ de l'audit attendu et de sa conduite. Il est réalisé conformément à des normes d'audit. Il comprend la description de l'approche d'audit ainsi que le planning. Il se compose de plusieurs missions de test durant une période donnée.*

Pour créer un plan :

1. Dans la barre de navigation, cliquez sur **Testing > Plans de test**.
2. Cliquez sur le bouton **Nouveau**.
   Le nouveau plan apparaît.
3. Ouvrez la fenêtre de propriétés du plan.
4. Dans l'onglet **Caractéristiques**, modifiez le **Nom** du plan.
5. Sélectionnez la **Nature** du plan :
   - Audit
   - Test
   - Conformité
   - Mixte

   > ☛ *Si vous disposez uniquement de **Hopex Internal Control**, la nature du plan est automatiquement renseignée et n'est pas modifiable.*
   >
   > ☛ *Selon la nature du plan sélectionnée, un onglet **Tests** et/ou **Audits** apparaîtra dans la fenêtre de propriétés du plan.*
   >
   > ☛ *Si vous avez sélectionné les valeurs "Test" ou "Mixte", une campagne d'évaluation est créée lors de la validation du plan. Elle va permettre de générer par la suite des questionnaires à destination des contrôleurs internes pour l'évaluation des contrôles. Pour plus de détails, voir Evaluer les contrôles.*
6. Sélectionnez le **Calendrier** du plan.
7. Modifiez éventuellement la **Date de début** et la **Date de fin**.

   > ☛ *Le **Statut** est défini de façon automatique par le workflow.*
8. Cliquez sur **Enregistrer**.

Le plan est créé.

Vous pouvez maintenant créer des missions de test directement dans la page du plan.

Planifier les missions de test

La planification des missions de test est réalisée par le Manager GRC.

📖 *Une mission de test est une mission assignée à un contrôleur dans le cadre d'un plan.*

Créer une mission de test

Pour créer une mission de test :

1. Cliquez sur **Testing > Plans de test**.
2. Ouvrez les propriétés du plan qui comprend la mission de test à créer.
3. Sélectionnez la page **Tests**.
4. Cliquez sur **Nouveau**.
   La nouvelle mission de test apparaît sous le plan.

☛ *Pour définir les caractéristiques de la mission de test, voir Définir les propriétés d'une mission de test.*

Accéder aux missions de test d'un plan de test

Pour accéder aux missions de test d'un plan de test :

- Cliquez sur **Testing > Plans de test**, et dépliez un plan.
  Les missions de test (ou missions d'audit, selon la nature du plan sélectionné) correspondant au plan déplié apparaissent.

Définir les propriétés d'une mission de test

Vous pouvez spécifier un certain nombre d'informations sur une mission de test.

Voir aussi Visualiser le tableau de bord d'une mission de test.

Caractéristiques générales

Les caractéristiques générales de la mission de test sont :

- **Nom** : nom de la mission de test.
- **Code** : vous pouvez donner un code à la mission de test
- **Incluse dans le plan initial** : cet attribut est défini automatiquement selon le statut du plan au moment de la création de la mission de test. Il

indique si la mission de test était présente à la création du plan ou si elle a été ajoutée ultérieurement.

- **Entité** contrôlée
- **Chef de mission** : nom du chef de la mission de test
- **Responsable de l'entité contrôlée**
- **Objectif** de la mission de test
- **Catégorie** de la mission de test :
  - "Conformité"
  - "Efficacité"
- **Etat** de la mission de test : cet attribut est défini automatiquement, et modifié lors d'une transition dans le workflow.

Motivations et charge

Dans cette section vous pouvez saisir les caractéristiques suivantes :

- **Origine** : suivi, ponctuelle, récurrente, etc.
- **Priorité** : des priorités peuvent être données aux missions de test. Vous pouvez sélectionner les missions de test à intégrer au plan sur la base de ce critère.
- **Durée estimée** (jours)
- **Ressources estimées**
- **Charge de travail estimée**

☛ *Les caractéristiques suivantes sont calculées automatiquement :*

- ***Charge effective (heures)*** *: calculée à partir de la charge effective définie sur les feuilles de temps ou sur les activités si aucune feuille de temps n'a été saisie.*
- ***Nombre de ressources affectées***

- **Justification** de la mission de test

Périmètre

Dans cette section vous pouvez relier des catégories de processus ou processus à la mission de test.

Ceux-ci peuvent être utilisés pour générer automatiquement le programme de travail de la mission de test.

☛ *Pour plus de détails, voir Compléter le programme de travail manuellement.*

Jalons

Dans cette section vous pouvez indiquer une **Date de début prévue** et une **Date de fin prévue**. Ces dates constituent les jalons de la mission.

☛ *Vous pouvez choisir de saisir les jalons plus tard.*

Utilisateurs

Dans cette section vous pouvez spécifier les intervenants d'une mission de test :

- **Contrôleur du test** : les contrôleurs ayant été préalablement définis, vous pouvez relier mais pas créer de contrôleur. Voir Affecter les ressources aux missions de test.
- **Personne testée**
- **Autre participant à la mission de test** (à titre informatif seulement)

Compétences

Dans cette section vous pouvez préciser les compétences dont les contrôleurs doivent disposer pour réaliser la mission de test.

Pour définir les compétences nécessaires à la mission de test :

1. Dépliez la section **Compétences**, cliquez sur **Nouveau** ou **Relier** pour créer une compétence ou relier une compétence existante.

Au moment d'affecter les contrôleurs à une mission de test, vous serez en mesure de comparer les compétences des contrôleurs et les compétences exigées par la mission de test. Pour plus de détails sur le rapport fournissant ces informations, voir Affecter les ressources aux missions de test.

Conclusion

Dans la section **Conclusion** vous pouvez spécifier :

- les **Points forts clés**
- les **Points faibles clés**
- une **Evaluation** : bon niveau, peut-être améliorée, etc.

> ☛ *La valeur de l'évaluation spécifiée ici apparaît dans le tableau de bord de la mission de test, en haut de l'onglet **Caractéristiques**.*

Activités de test

Une page spécifique dans les propriétés de la mission de test permet de visualiser les activités de test.

Défaillances

Une page spécifique dans les propriétés de la mission de test permet de visualiser les défaillances.

Visualiser le tableau de bord d'une mission de test

Pour accéder au tableau de bord d'une mission de test :

1. Voir Accéder aux missions de test d'un plan de test.
2. Ouvrez les propriétés d'une mission de test.

La page **Caractéristiques** affiche un tableau de bord qui présente des informations essentielles concernant la mission de test :

- % d'**Avancement** = nombre d'activités de test en statut "fermé" / nombre total d'activités de test de la mission de test
- **Evaluation** de la mission de test:
  - bon niveau
  - peut être améliorée
  - etc.

    ☛ *Cette évaluation est réalisée par le directeur de l'audit.*
- **Défaillances** : affiche le nombre de défaillances

Créer des missions de test "modèles"

Les missions de test "modèles" sont des programmes de travail qui sont préparés spécialement pour être appliqués à de nouvelles missions de test.

Ce statut est réservé aux missions de test d'un plan de test qui est lui-même défini comme modèle. Il s'applique automatiquement aux missions de test existantes du plan de test modèle et est proposé lors de la création d'une nouvelle mission de test sur ce même plan de test.

Pour définir un plan de test comme modèle :

1. Cliquez sur **Testing > Plans de test**.
   La liste des plans apparaît.
2. Cliquez sur l'icône du plan en question et sélectionnez **A valider > Définir comme modèle**.

Décider des missions de test à réaliser

Visualiser le rapport de couverture des missions de test

Hopex GRC fournit un rapport donnant des informations sur le nombre de missions de test réalisées sur chaque entité entre deux dates. Il permet de se rendre compte des entités qui ont besoin d'être testées et de générer les missions de test correspondantes.

Pour accéder à ce rapport :

1. Cliquez sur **Testing > Préparation > Couverture des entités**.
2. Dans la fenêtre d'édition, sélectionnez une date de début et de fin.
3. (optionnel) Sélectionnez le score obtenu par la mission de test ou son statut.

Pour chaque entité testée le rapport présente :

- Le **Nombre de tests** réalisés entre les deux dates (date de début et de fin effectives)
- La **Date de fin** du dernier test (date de fin effective), ou son état s'il est toujours en cours
- Le nom du **Dernier test**
- Le **Score** du dernier test

Pour générer les missions de test correspondant à une ou plusieurs entités :

- Sélectionnez l'entité ou les entités qui vous intéressent puis cliquez sur le bouton **Générer des missions de test**.
  Un assistant vous demande de choisir un plan cible. Les missions de test sont générées.

Visualiser les dépenses des missions passées

Un rapport vous permet de visualiser les dépenses des missions passées.

Pour accéder à ce rapport :

1. Cliquez sur **Testing > Plans de test**.
2. Sélectionnez un plan et dans sa fenêtre de propriétés, sélectionnez la page **Rapports**.
3. Dans la liste déroulante, sélectionnez **Dépenses**.

Vous pouvez visualiser les frais :

- par catégorie
- par ressource (auditeur, contrôleur ou testeur).

Sélectionner les missions de test à intégrer au plan de test

Les missions de test créées sont actives uniquement après validation. Parmi toutes les missions de test, certaines font partie du plan définitif ; d'autres sont rejetées.

Hopex GRC propose des outils facilitant la sélection des missions de test à intégrer au plan.

Rejeter des missions de test

Les missions de test potentielles jugées non prioritaires peuvent être rejetées via le workflow.

Pour rejeter une mission de test :

- Cliquez sur l'icône de la mission de test à rejeter et sélectionnez **A valider > Rejeter**.

La mission de test est rejetée mais non supprimée. Elle pourra servir de modèle pour une nouvelle mission de test l'année suivante.

Valider les missions de test

Vous pouvez valider les missions de test :

- globalement, lors de la validation du plan de test.
- individuellement

Planifier les missions de test via un diagramme de Gantt

Un rapport permet au directeur du contrôle interne (ou Manager GRC) de planifier les différentes missions de test d'un plan de test.

Pour afficher ce rapport :

1. Sous **Testing** > **Plans de test**, ouvrez les propriétés du plan en question.

2. Sélectionnez la page **Planification**.
   Un diagramme de Gantt décrit les missions du plan.

Par défaut la planification porte sur l'année en cours. Vous pouvez visualiser des missions sur une période plus précise.

Pour redéfinir la période d'affichage du diagramme de Gantt :

- sélectionnez une période de calendrier, ou
- une date de début et de fin spécifique.

Pour modifier les dates d'une mission dans le diagramme :

- Cliquez au centre de période et déplacez la souris pour déplacer simultanément la date de début et le date de fin.

Affecter les ressources aux missions de test

Avant d'affecter une ressource à une mission de test, vous pouvez visualiser sa disponibilité et ses compétences.

Visualiser la disponibilité des ressources

Pour visualiser les ressources disponibles et compétentes pour une mission de test :

1. Ouvrez la fenêtre de propriétés du plan de test concerné.
2. Sélectionnez la page **Affectation des ressources**.

   ☛ *Par défaut le rapport présente les missions de test du plan de test sur l'année. Vous pouvez afficher ceux d'une période en particulier.*
3. Dans le tableau supérieur gauche, sélectionnez une mission de test.
4. Dans le tableau supérieur droit, sélectionnez une ressource dont vous souhaitez afficher la disponibilité.

   ☛ *Vous pouvez sélectionner plusieurs ressources.*
5. Dans le cadre inférieur, cliquez sur le bouton **Rafraîchir**.

Deux graphes présentent :

- Les compétences exigées par la mission de test et les compétences de la ressource sélectionnée.
- La disponibilité de la ressource aux dates de la mission de test.
  La couleur de la période de la mission de test est fonction du nombre de ressources qui lui sont affectées par rapport au nombre de ressources estimé :
  - Vert si la mission de test dispose de ressources en nombre suffisant
  - Jaune si elle manque des ressources
  - Rouge si aucune ressource ne lui est affectée

    ☛ *Ce deux graphes doivent être rafraîchis séparément.*

Affecter une ressource à une mission de test

Pour affecter une ressource à une mission de test :

1. Dans la page **Affectation des ressources** de la fenêtre de propriétés d'un plan de test, dans le cadre supérieur gauche, sélectionnez la mission de test désirée.

2. Dans le cadre supérieur droit, sélectionnez une personne et cochez la case **Affecter**.

   ☛ Pour enlever une affectation, *effectuez la même opération et décochez la case **Affecter**.*

Spécifier un chef de mission pour une mission de test donnée

Pour renseigner le chef de mission sur une mission de test :

1. Ouvrez la fenêtre de propriétés de la mission de test concernée.
2. Renseignez le champ **Chef de mission**.

Envoyer la lettre de notification

Après avoir complété les renseignements nécessaires à la réalisation de la mission de test, le directeur du contrôle interne peut envoyer une lettre de notification qui informe les personnes contrôlées de la mission de test.

L'envoi d'une lettre de notification n'est pas incluse dans le workflow. Elle précède l'étape du workflow qui consiste à publier la mission de test.

Créer la lettre de notification

Pour créer la lettre de notification de la mission de test :

- Cliquez sur l'icône de la mission de test et sélectionnez **Livrables > Lettre de notification**.
  Un message vous demande si vous souhaitez ouvrir ou enregistrer le fichier. Le document présente le commentaire saisi dans les caractéristiques de la mission de test.

Une fois le document enregistré, vous pouvez l'ouvrir et le modifier.

Vous pouvez également le relier à la mission de test en tant que document métier, sous la catégorie "Lettre de notification". Pour plus de détails, voir Utiliser les documents métier.

Relier la lettre de notification à la mission de test

Le fichier est généré à partir du contenu de la mission de test mais n'est pas relié par défaut à la mission de test.

Pour relier la lettre de notification à la mission de test :

1. Ouvrez les propriétés de la mission de test.
2. Sélectionnez la page **Documents** et l'onglet **Documents métier**.
3. Glissez-déplacer la lettre de notification préalablement générée.
   Le document apparaît dans la liste des documents attachés à la mission de test.
4. Ouvrez les propriétés du document et dans le champ **Catégorie de document**, sélectionnez "Lettre de notification".

Valider la mission de test

Lorsque le directeur du contrôle interne décide qu'une mission de test doit être exécutée au cours du plan de test, il valide la mission de test.

> ☛ *Une session d'évaluation est créée. Elle va permettre de générer par la suite des questionnaires à destination des contrôleurs internes pour l'évaluation des contrôles. Pour plus de détails, voir Evaluer les contrôles.*

Publier la mission de test

Hopex GRC permet de préparer les missions de test et de ne les rendre publiques aux contrôleurs que lorsque la planification est terminée.

Pour rendre publique une mission de test :

1. Cliquez avec le bouton droit sur l'icône de la mission de test.
2. Sélectionnez **A publier** > **Publier**.

Le statut de la mission de test passe à "Publié".

Une fois publiées, les missions de test apparaissent dans le programme de travail des contrôleurs.

Préparer les missions de test

La supervision du déroulement d'une mission de test est assurée par le chef de mission. Dans la phase de préparation de la mission, il établit le programme de travail et affecte les activités aux contrôleurs.

Pré-requis à l'élaboration d'un programme de travail

Pour que le programme de travail puisse être généré :

- des catégories de processus ou processus doivent être reliés à l'entité
- des contrôles doivent être reliés aux catégories de processus/processus

Contenu du programme de travail

Hopex GRC permet de créer automatiquement une structure de programme de travail à partir :

- de l'arborescence des processus reliés à l'entité, ou
- des processus spécifiés dans le périmètre de la mission de test

> ☛ *Si aucun processus n'a été spécifié dans la périmètre de la mission de test, tous les processus reliés à l'entité figureront dans le programme de travail.*

Objets de l'environnement	Objets créés dans le programme de travail
Catégorie de processus ou processus	Thème de test
Contrôle (relié à la catégorie de processus ou au processus)	Activité de test

> ☛ *L'entité est représentée par la mission de test.*

Thème de test

Un thème correspond à une catégorie de processus ou à un processus.

Les thèmes sont utilisés pour regrouper les activités de test et les fiches de travail, c'est-à-dire organiser le contenu de la mission de test.

Activité de test

Une activité de test correspond à un contrôle.

Il s'agit de l'élément de base de la mission de test. C'est elle qui permet d'affecter la responsabilité au contrôleur.

Fiche de travail

Une fiche de travail est constituée de points à vérifier sur un sujet donné au cours d'une activité d'audit.

Une fiche de travail est générée pour chaque activité de test générée. Pour plus de détails, voir Créer une fiche de travail.

Accéder aux mission de test à préparer

Pour accéder aux missions de test à préparer :

❱ Dans la barre de navigation, cliquez sur **Testing > Exécution > Global**.

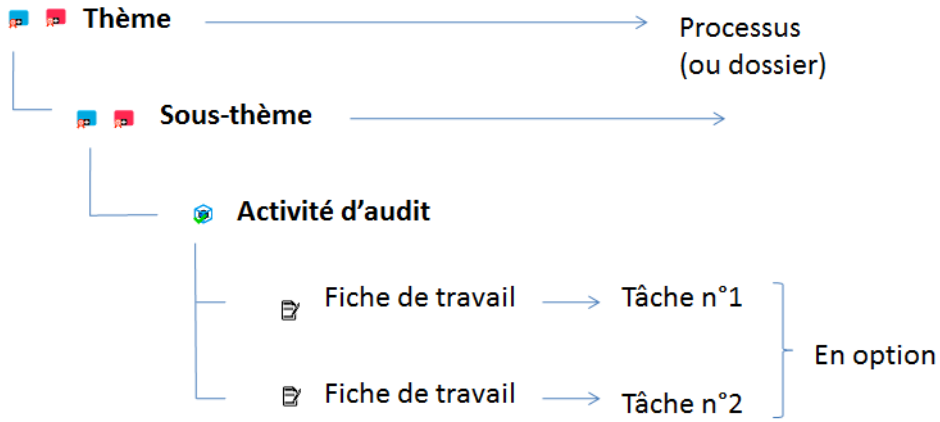
Créer un programme de travail automatiquement

Pour constituer un programme de travail automatiquement :

1. Voir Accéder aux mission de test à préparer.

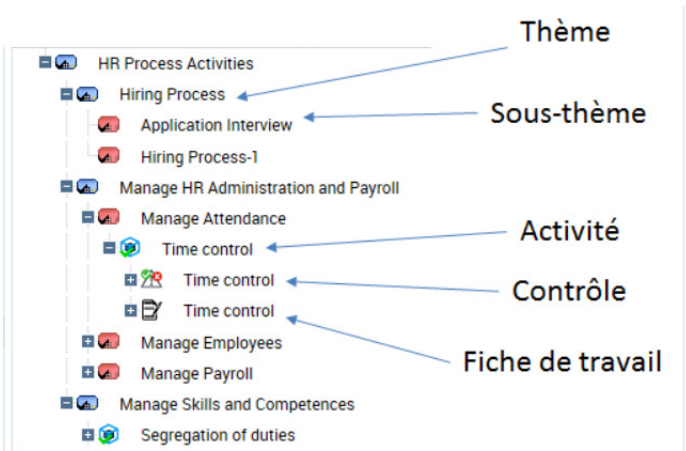
2. Cliquez sur l'icône de la mission de test et sélectionnez **Générer le programme de travail**.
   Cette commande va dupliquer l'arborescence des catégories de processus/processus pour l'entité dans le périmètre de la mission de test.

Si des processus sont spécifiés explicitement dans le périmètre de la mission de test, seuls ces processus sont créés automatiquement dans la structure du programme de travail.



Compléter le programme de travail manuellement

Le chef de mission peut compléter la mission de test manuellement pour préciser son contenu. Il peut ajouter ou enlever des thèmes / activités dans la page **Programme de travail** de la mission de test.



Créer un thème

Pour créer un thème :

1. Dans la page **Programme de travail** des propriétés d'une mission de test, cliquez sur un thème généré automatiquement et sélectionnez **Nouveau > Thème de test**.
2. Affichez les propriétés du thème.
   Vous pouvez :
   - sélectionner un thème de test parent (si vous souhaitez créer une arborescence de thèmes).
   - relier le thème de test à un processus (**Périmètre du thème**).
   - saisir un commentaire.

Vous pouvez visualiser l'arborescence des thèmes/sous-thèmes ainsi créée. Vous pouvez maintenant créer des activités et des fiches de travail.

Créer une activité

Une activité de test est un élément d'une mission qui porte sur un contrôle.

Pour créer une activité :

1. Dans la page **Programme de travail** des propriétés d'une mission de test, cliquez sur un thème et sélectionnez **Nouveau > Activité de test**.
2. Affichez les propriétés de l'activité.
3. Reliez l'activité de test à un **Contrôle**.
4. Sélectionnez le **Responsable** de l'activité de test, qui peut être un contrôleur ou le chef de mission de la mission de test courante.
5. Indiquez la **Charge de travail estimée**.

> ☛ *Vous pouvez ultérieurement saisir manuellement la charge de travail effective sur cette activité.*

Affecter les activités

Affecter une activité

Le chef de mission spécifie pour chaque activité :

- les dates de début et de fin
- la charge de travail estimée
- le contrôleur chargé de sa réalisation

Pour saisir ces données :

1. Dans la fenêtre de propriétés de la mission de test, sélectionnez la page **Activités**.
2. Ouvrez la fenêtre de propriétés de l'activité de test concernée.
3. Dans le champ **Responsable**, à l'aide de la flèche tournée vers la droite sélectionnez un contrôleur parmi les contrôleurs candidats.
4. Saisissez les dates de début et de fin de l'activité de test.
5. Spécifiez la charge de travail.

Affecter plusieurs activités à un même contrôleur

Pour affecter plusieurs activités à un même contrôleur :

1. Dans la fenêtre de propriétés de la mission de test, sélectionnez la page **Activités**.
2. Sélectionnez plusieurs activités et cliquez sur le bouton **Assignation**.
3. Dans l'assistant d'assignations multiples, sélectionnez le **Propriétaire de l'activité de test**.
4. Cliquez sur **OK**.

Procéder à la revue du programme de travail

Le chef de mission peut générer un rapport sur son programme de travail. Ce rapport lui permet de vérifier que :

- l'affectation des tâches a été réalisée correctement
- le programme de travail traite des risques et processus appropriés

Consulter le rapport du programme de travail

Pour accéder au rapport du programme de travail :

- Dans la page de la mission de test, sélectionnez **Rapports** > **Programme de travail**.

Vous pouvez visualiser :

- la comparaison des ressources allouées et les ressources disponibles
- la charge de travail (en jours-homme)
- la charge de travail par thème (en jours-homme)
- les activités par thème

Exporter le programme de travail sous Excel

Le programme de travail sous Excel reprend les thèmes, sous-thèmes, activités et fiches de travail.

Le fait d'avoir à disposition le programme de travail sous Excel permet de :

- consulter l'ensemble du programme de travail sans avoir à accéder aux objets individuellement
- stocker une version imprimée du programme de travail
- visualiser les tâches à effectuer lors du signalement d'une défaillance

Pour exporter le programme de travail :

- Dans la page **Programme de travail** de la mission de test, faites un clic droit à la racine de l'arborescence et sélectionnez **Livrables > Export du programme de travail (Excel)**.

  ☛ *Une fenêtre pop-up s'ouvre en bas de la page. Si votre navigateur bloque ces fenêtres, vous ne pouvez pas voir l'export du fichier. Dans ce cas désactivez le blocage des fenêtres pop-up dans le navigateur.*

Vous pouvez modifier le programme de travail dans Excel.

Une fois le programme de travail modifié, vous pouvez créer un document métier dans **Hopex GRC** et réimporter le programme de travail modifié.

Pour créer le document métier correspondant au programme de travail modifié :

1. Dans la fenêtre de propriétés de la mission de test, sélectionnez la page **Documents**.
2. Sélectionnez l'onglet **Document métier** et glissez-déplacez le document Excel du programme de travail.
   Le programme de travail modifié est maintenant stocké dans le référentiel **Hopex**.

   ☛ *Dans la fenêtre de propriétés du document métier créé, vous pouvez préciser la **Catégorie de document** "Programme de travail".*

   ☛ *Pour plus de détails, voir Utiliser les documents métier.*

Valider le programme de travail

Lorsque le chef de mission valide le programme de travail via le workflow, une session d'évaluation est automatiquement créée et reliée à la mission de test. Des questionnaires d'évaluation sont générés et rendus disponibles à partir des activités de test. Les répondants sont les propriétaires des activités de test.

☛ *Pour plus de détails, voir Evaluer les contrôles.*

Pour valider le programme de travail :

- Cliquez sur l'icône de la mission de test et sélectionnez **A valider** > **Valider**.

Effectuer des tâches d'ordre administratif

Planifier les ressources

Les contrôleurs peuvent être affectés à différentes missions en même temps. Il est important de saisir le temps alloué pour chacun à une mission.

Pour indiquer sur chaque contrôleur le temps à consacrer à une mission :

1. Dans la fenêtre de propriétés de la mission, dépliez la section **Responsabilités**.
2. Cliquez sur l'onglet **Contrôleur de test**.
3. Sélectionnez un utilisateur et dans le champ **Charge (en heures)**, saisissez le temps qu'il doit passer sur la mission.

Créer des tâches d'ordre général

Le directeur peut créer pour les contrôleurs des tâches non directement liées aux missions.

Pour créer une tâche générale :

1. Cliquez sur **Testing > Préparation > Tâches générales**.
2. Renseignez des dates, un commentaire et reliez des utilisateurs à cette tâche.
   Les utilisateurs affectés à cette tâche peuvent imputer des heures sur cette tâche dans leur feuille de temps.

Valider les congés

Pour faire apparaître les congés dans les feuilles de temps des auditeurs, vous devez avoir au préalable valider le congé.

Pour valider le congé :

1. Cliquez sur **Testing > Préparation > Demandes de congés** et ouvrez la fenêtre de propriétés du congé à valider.
2. Positionnez son statut à "Validé".

Initialiser des notes de frais

Le chef de mission peut créer une note de frais par auditeur/contrôleur pour tous les auditeurs/contrôleurs affectés à la mission. Il s'agit dans ce cas d'initialiser les notes de frais.

Pour initialiser les notes de frais :

1. Dans la fenêtre de propriétés d'une mission, sélectionnez la page **Dépenses**.
2. Cliquez sur le bouton **Initialiser**.
   Une note de frais est créée pour chaque auditeur/contrôleur.

Pour créer une dépense :

1. Dans la fenêtre de propriétés de la note de frais, dépliez la section **Dépenses** et cliquez sur **Nouveau**.
2. Saisissez pour chaque dépense :
   - un **Montant**
   - une **Date**
   - la **Catégorie de dépense** : "Logement", "Nourriture et boissons", "Transport"
   - éventuellement un **Commentaire**

> ☛ *L'auditeur saisit le montant dans la devise qu'il souhaite. Le montant converti est calculé automatiquement.*

EXÉCUTER LES MISSIONS DE TEST

> ☛ *Les manipulations décrites ici concernent le profil "Contrôleur interne" seulement.*

L'élaboration du programme de travail d'une mission de test permet aux contrôleurs internes :

- d'exécuter des tests sur échantillon via des fiches de test

  > ☛ *Ces fiches de test se présentent sous la forme de check-lists. Les questions sont posées pour chaque objet présent dans l'échantillon constitué.*

- d'évaluer les contrôles en termes de conception et d'efficacité via des questionnaires

  > ☛ *Il s'agit des mêmes questionnaires que ceux abordés au chapitre concernant les campagnes d'évaluation.*

Prendre connaissance du programme de travail

Le contrôleur interne a besoin de consulter son programme de travail.

Pour accéder aux tâches à réaliser :

❱ A partir de la barre de navigation, sélectionnez **Testing > Exécution > Mes activités**.

Exécuter les tests sur échantillon

Les contrôleurs internes exécutent sur des échantillons les étapes de test définies sur les contrôles.

Pour pouvoir compléter la fiche de test, vous devez avoir au préalable :

- généré ou créé des fiches de travail
- spécifié ou modifié la taille de l'échantillon de test
- généré l'échantillon de test
- défini les questions des fiches de test

Créer une fiche de travail

Les *fiches de travail* sont des dossiers ou papiers de travail qui servent de base au contrôleur dans la réalisation de la mission de test.

> ☛ *Les fiches de travail sont créées automatiquement lors de la génération du programme de travail. Pour plus de détails, voir Contenu du programme de travail.*

Pour créer une fiche de travail manuellement :

1. Dans les propriétés d'une mission de test, sélectionnez la page **Programme de travail**.
2. Sélectionnez l'activité concernée et affichez ses propriétés.

3. Dans la page **Caractéristiques** de l'activité, section **Fiches de travail**, cliquez sur le bouton **Nouveau**.
   La fiche de travail apparaît :
   - dans la page de l'activité de test
   - dans l'arborescence du programme de travail de la mission de test.
4. Dans le programme de travail, sélectionnez la fiche pour faire apparaître ses **Propriétés**.
5. Saisissez un nom ainsi que vos commentaires.
6. Cliquez sur **OK**.

Spécifier ou modifier la taille de l'échantillon

Le contrôleur doit spécifier la taille de l'échantillon de la mission de test sur la fiche de travail. Il s'agit du nombre d'éléments à tester.

Pour spécifier la taille de l'échantillon :

1. Dans les propriétés de la mission de test, sélectionnez la page **Programme de travail**.
2. A partir du programme de travail, ouvrez la fenêtre de propriétés d'une fiche de travail.
3. Renseignez le champ **Taille de l'échantillon**.
   Il s'agit de la taille de l'échantillon choisi pour le testing.

> ☛ *Par défaut la valeur est héritée de la taille de l'échantillon spécifiée sur le contrôle. Pour plus de détails, voir Définir les questions des fiches de test.*

Générer l'échantillon de test

L'échantillon de test est généré directement à partir des informations disponibles sur le contrôle (étapes de test).

Pour générer l'échantillon de test :

1. Dans les propriétés de la mission de test, sélectionnez la page **Programme de travail**.
2. A partir de l'arborescence du programme de travail, cliquez sur l'icône d'une fiche de travail et sélectionnez **Générer l'échantillon de test**.
   En fonction de la taille de l'échantillon spécifiée au préalable, un message vous informe du nombre d'éléments qui vont être créés dans l'échantillon de test.
   L'échantillon de test généré est disponible dans la fenêtre de propriétés de la fiche de travail.

Définir les questions des fiches de test

Les fiches de travail contiennent des fiches de test, qui présentent sous forme de tableau les points à exécuter. Ces fiches de test contiennent :

- en ligne, les éléments de l'échantillon à contrôler
- en colonne, les questions (représentées par les étapes de test)

Vous devez définir les questions de la check-list avant de pouvoir générer des fiches de test.

> ☛ *Pour plus de détails, voir Préparer le test des contrôles.*

Renseigner les fiches de test générées

Pour pouvoir visualiser les fiches de test, vous devez avoir au préalable :

- défini les questions des fiches de test

  ☛ *Voir Définir les questions des fiches de test*

- généré l'échantillon de test

  ☛ *Voir Générer l'échantillon de test*

Pour visualiser la fiche de test :

1. Dans les propriétés de la mission de test, sélectionnez la page **Programme de travail**.
2. Ouvrez la fenêtre de propriétés de la fiche de travail qui vous intéresse.
3. Sélectionnez l'onglet **Fiche de test**.
   Cette fiche de test présente :
   - en ligne, les éléments de l'échantillon de test à contrôler
   - en colonne, les étapes de test

Vous pouvez répondre aux questions posées dans les colonnes prévues à cet effet.

Evaluer une activité de test

Après avoir renseigné les fiches de test, le contrôleur peut évaluer l'activité de test globalement.

☛ *Cette évaluation à dire d'expert se base ou non sur les résultats produits par les fiches de test.*

Pour évaluer l'activité de test :

1. Ouvrez la fenêtre de propriétés de l'activité de test.
2. Dans le champ **Résultat du test**, précisez si la mission a :
   - échoué
   - réussi
   - n'a pas encore été évaluée

Évaluer les contrôles

Les contrôleurs internes doivent évaluer les contrôles en termes de conception et d'efficacité.

☛ *Cette évaluation fait appel à la mécanique standard des campagnes d'évaluation. Les questionnaires générés sont à distinguer de ceux correspondant aux fiches de test.*

Génération des questionnaires

Les questionnaires sont générés lors de la validation du programme de travail.

☛ *Pour plus de détails, voir Valider le programme de travail.*

Répondre aux questionnaires

Vous pouvez répondre aux questionnaires d'évaluation des contrôles :

- sur une mission de test
- sur chaque activité de test d'une mission de test

Pour visualiser les questionnaires d'une mission de test :

1. Dans la barre de navigation, cliquez sur **Testing > Plans de test**.
2. Dans la fenêtre de propriétés d'une mission de test, dépliez la section **Evaluation**.
3. Sélectionnez un questionnaire et cliquez sur **Afficher les questionnaires**.
4. Sélectionnez tour à tous les questions et répondez-y dans la partie inférieure de la fenêtre.
5. Cliquez sur **Enregistrer**.

Pour visualiser les questionnaires d'une activité de test :

1. Dans la fenêtre de propriétés d'une mission de test, sélectionnez la page **Programme de travail**.
2. Dans le menu contextuel d'une activité de test, sélectionnez **Evaluation**.

Gérer son temps et ses dépenses

Gérer ses dépenses

Les auditeurs/contrôleurs affectés à une mission peuvent créer des notes de frais sur cette même mission. Dans ce cas ils doivent soumettre leur note de frais au chef de mission via un workflow.

Pour créer une note de frais :

1. Dans la barre de navigation, sélectionnez **Testing > Temps et dépenses > Dépenses**.
2. Cliquez sur **Nouveau**.
3. Dans le champ **Détenteur**, sélectionnez la mission concernée.

   ☛ *Vous pouvez également créer une note de frais dans la page **Dépenses** de la fenêtre de propriétés d'une mission. Dans ce cas, vous n'avez pas besoin de spécifier la mission détentrice.*
4. Cliquez sur **OK**.
   Une note de frais est créée. Vous allez maintenant créer les dépenses associées.
5. Dans la section **Dépenses** de la fenêtre de propriétés de la note de frais, cliquez sur **Nouveau**.

6. Dans la fenêtre de propriétés de la note de frais, saisissez un **Montant** ainsi qu'une **Date** : vous pouvez saisir le montant dans la devise que vous souhaitez (parmi celles auxquelles vous avez accès).

☛ *Le montant est converti dans la devise qui a été paramétrée pour votre utilisateur.*

7. Spécifiez éventuellement :
   - la **Catégorie de dépense** : "Logement", "Nourriture et boissons", "Transport"
   - un **Commentaire**
8. Cliquez sur l'icône de la note de frais et soumettez-là éventuellement via le workflow.

☛ *Le chef de mission n'a pas besoin de faire approuver ses notes de frais.*

☛ *Vous pouvez exporter vers Excel les données contenues dans la note de frais.*

Saisir des congés

La saisie des congés permet de :

- mieux planifier les campagnes de test.
- pré-remplir les feuilles de temps.

Pour saisir un congé:

1. Dans la barre de navigation, sélectionnez **Testing > Temps et dépenses > Demandes de congés**.
2. Cliquez sur **Nouveau**.
3. Dans la fenêtre de propriétés, sélectionnez un **Plan** de rattachement.
4. Spécifiez également :
   - le **Type de congé** (vacances, formation, autre)
   - les dates de début et de fin prévues et effectives.
   - un commentaire éventuel
5. Dans le champ **Statut**, sélectionnez "Soumis".

☛ *Pour que le congé apparaisse dans la feuille de temps, le chef de mission doit avoir validé le congé (en positionnant la valeur du statut à "Validé").*

☛ *Un auditeur/contrôleur peut modifier ou supprimer un congé tant que ce congé n'a pas été validé.*

Remplir une feuille de temps

Les auditeurs/contrôleurs peuvent remplir des feuilles de temps dans le cadre de leur mission.

Pour remplir une feuille de temps :

1. Dans la barre de navigation sélectionnez **Testing > Temps & dépenses > Feuilles de temps**.
   La feuille de temps affiche une ligne par mission.
2. Saisissez pour chaque jour le nombre d'heures passées sur chaque mission.
3. Cliquez sur **Soumettre** pour enregistrer votre feuille de temps.
4. Cliquez sur **Suivant** pour saisir vos heures concernant la semaine suivante.

> ☛ *Des messages peuvent apparaître si le compte rendu d'activité est incohérent. Par exemple si des heures ont été imputées sur une mission alors que la mission n'a pas démarré. Vous pouvez toutefois soumettre une feuille de temps incomplète.*

La feuille de temps permet de saisir pour chaque jour et pour chaque semaine le nombre d'heures passées sur chaque mission.

> ☛ *Seules les missions qui ont été publiées sont visibles dans la feuille de temps.*

La feuille de temps fait également apparaître :

- les congés qui ont été validées
- les tâches générales (réunions, formation, gestion d'équipe, administration ...)

Gérer les défaillances et plans d'action

Le contrôleur complète le programme de travail par la saisie de :

- défaillances
- plans d'action

Gérer les défaillances

Créer une défaillance

Pour créer une défaillance :

1. Dans la barre de navigation, sélectionnez **Testing > Traitement > Défaillances**.
2. Cliquez sur **Nouveau**.

Dans les propriétés d'une défaillance vous pouvez qualifier son **Impact**.

> ☛ *Les défaillances sont également accessibles dans le programme de travail et dans les propriétés de l'activité de test.*

Enregistrer les preuves de test

Vous pouvez lier des documents ou spécifier une adresse URL pour illustrer une défaillance.

Pour ajouter un document en pièce jointe :

1. Dans l'arborescence du programme de travail d'une mission de test, sélectionnez une défaillance sur laquelle vous souhaitez ajouter un document.

2. Dépliez la section **Pièces jointes**.
3. Dans l'onglet **Document métier**, glissez-déplacez un document.

> 🕮 *Un document métier est un document dont le contenu est indépendant du référentiel. Ce document peut être un fichier MS Word, MS Powerpoint ou autres. Un rapport (MS Word) généré sur un objet peut devenir un document métier.*

Le document apparaît dans la liste des documents attachés à la défaillance. Il est détenu par la mission de test de la défaillance. Vous pouvez donc le voir apparaître également dans l'onglet **Documents** de la mission de test.

> ☛ *Pour plus de détails, voir Utiliser les documents métier.*

Gérer les plans d'action

Les plans d'action peuvent être créés à partir des défaillances.

Pour créer un plan d'action :

- Dans la page des propriétés d'une défaillance, sélectionnez la page **Plans d'action** et cliquez sur **Nouveau**.
  Le plan d'action apparaît dans la section.

Superviser la mission de test

Le chef de mission doit valider les travaux des contrôleurs via le workflow d'activité.

Ensuite il peut contrôler leurs travaux et assurer le suivi de la mission de test. Pour lui faciliter la tâche, des rapports permettant de contrôler la mission de test sont disponibles sur chacune d'elle.

Rapports de contrôle d'une mission de test

Pour accéder aux rapports de contrôle d'une mission de test :

- Dans la page de la mission de test, sélectionnez la page **Rapports > Supervision**.

Trois rapports apparaissent :

- **Objectivité des défaillances** : afin d'assurer l'objectivité des défaillances, des preuves doivent être apportées.
  Le chiffre qui est affiché représente le pourcentage des défaillances ayant au moins une pièce jointe.
- **Avancement des travaux par contrôleur**
- **Tableau de synthèse** d'activité des contrôleurs

Rapports de suivi des feuilles de temps

Des rapports permettent de suivre les feuilles de temps des auditeurs/contrôleurs.

> ☛ *Ces rapports sont disponibles pour les managers Conformité seulement.*

Pour y accéder :

- Dans la barre de navigation, sélectionnez **Testing > Temps & dépenses > Suivi des feuilles de temps**.

Rapports des dépenses d'une mission de test

Pour visualiser les dépenses d'une mission :

- Dans la fenêtre de propriétés d'une mission de test, sélectionnez la page **Rapports > Dépenses de la mission de travail**.

Des diagrammes circulaires présentent la répartition des dépenses :

- par ressource (auditeur)
- par catégorie :
  - Nourriture et boissons
  - Logement
  - Transport

Pour visualiser la liste des dépenses associées à un secteur du diagramme :

- Faites un clic dans un secteur du diagramme circulaire.
  Les dépenses correspondantes apparaissent en liste dans la partie inférieure de la fenêtre.

Conclure la mission de test

Rapports d'évaluation de la mission de test

Des rapports permettent au chef de mission de mieux évaluer la mission de test et d'analyser ses plans d'action.

Pour y accéder :

- Dans la fenêtre de propriétés d'une mission de test, sélectionnez la page **Rapports > Evaluation**.

Plusieurs rapports sont proposés :

- Contrôles (réussite, échec, non évalué)
- Répartition des plans d'action par priorité (basse, haute, moyenne)
- Tableau de synthèse des éléments ci-dessus
- Défaillances recensées par thème

Générer le rapport de la mission de test

Le rapport de la mission de test reprend les éléments cette mission de test.

Pour générer le rapport d'une mission de test :

1. Dans la page de propriétés d'une mission de test, sélectionnez la page **Programme de travail**.

2. Cliquez sur l'icône de la mission de test et sélectionnez **Livrables > Rapport de la mission de test**.
   Un message vous demande si vous souhaitez ouvrir ou enregistrer le fichier.
3. Enregistrez le fichier afin de pouvoir le modifier et le soumettre par la suite.

Evaluer la mission de test

Pour évaluer la mission de test :

1. Dans la page **Caractéristiques** des propriétés de la mission de test, dépliez la section **Conclusion**.
2. Indiquez éventuellement :
   - les **Points forts clés** de la mission de test
   - les **Points faibles clés** de la mission de test
3. Dans le champ **Evaluation**, renseignez une valeur parmi :
   - "Bon niveau"
   - "Peut être améliorée"
   - "Amélioration nécessaire"
   - "A risque"

Terminer la mission de test

Lorsque la mission de test est fermée :

- le rapport de la mission de test est envoyé aux personnes qui ont été interviewées.
- les plans d'action sont envoyés à leur propriétaire.

Fermer la mission de test

Une fois la mission de test terminée, le directeur du contrôle interne peut fermer celle-ci.

☛ *Le fait de fermer la mission a pour effet de fermer tous les objets de niveau inférieur, à l'exception des plans d'action et actions. Une fois ces objets fermés, vous ne pouvez plus les modifier.*

☛ *L'administrateur peut exceptionnellement rouvrir ces objets si besoin.*

SUIVRE LES MISSIONS DE TEST

Mettre en œuvre des plans d'action

Accéder à vos plans d'action

Pour accéder à vos plans d'action :

- Dans la barre de navigation, sélectionnez **Plans d'action > Plans d'action > Plans d'action mettre en œuvre**.
  Cette liste présente les plans d'action qui vous ont été affectés.

Mettre en oeuvre des actions

Le propriétaire du plan d'action doit créer des actions.

Créer des actions

Pour créer une action :

1. Ouvrez les propriétés d'une mission de test.
2. Dans la page **Plans d'action**, cliquez sur un plan d'action pour ouvrir ses propriétés.
3. Dans la section **Actions**, cliquez sur **Nouveau**.
4. Ouvrez les propriétés de l'action créée.
5. Modifiez éventuellement son nom, saisissez une date limite ainsi qu'un responsable d'actions.
6. Cliquez sur **OK**.

Envoyer ou soumettre le plan d'action

Les actions créées et affectées aux utilisateurs appropriés constituent un plan d'action.

Pour soumettre le plan d'action :

- Cliquez avec le bouton droit sur le nom du plan d'action et sélectionnez **A envoyer** > **Envoyer**.

L'approbateur valide le plan d'action en retour.

> ☛ *Par défaut l'approbateur est le contrôleur qui a créé le plan d'action.*

Suivre la mise en place des plans d'action

Une fois le plan d'action validé par l'approbateur, les actions sont mises en œuvre par les personnes concernées.

Spécifier l'avancement des plans d'action

Le responsable du plan d'action est amené à tenir au courant l'approbateur du déroulement de ses actions.

Pour indiquer l'avancement d'un plan d'action:

1. Dans la page de propriétés d'un plan d'action, dépliez la section **Avancement du plan d'action**
2. Cliquez sur le bouton **Nouveau**.
   Un état d'avancement est créé.
3. Dans le champ **Pourcentage d'avancement**, précisez un pourcentage de réalisation du plan d'action.
4. Saisissez éventuellement un commentaire.
5. Cliquez sur **OK**.

> ☛ *Plusieurs états d'avancement peuvent être créés à des dates différentes.*

Suivre l'avancement d'un plan d'action

Après une période déterminée, le directeur du contrôle interne ou le chef de mission peuvent demander à recevoir des informations sur l'évolution des plans d'action.

Pour suivre l'avancement du plan d'action :

- Dans la page de propriétés du plan d'action, sélectionnez la page **Rapport d'avancement**.

Suivre les plans de test

Hopex GRC permet de suivre les plans de test en fonction de différents critères.

Afficher les rapports de suivi d'un plan de test

Des rapports permettent de suivre l'exécution du plan de test.

Pour accéder aux rapports du plan de test:

1. Ouvrez les propriétés du plan.
2. Sélectionnez la page **Rapports du plan**.

Supervision

Ce rapport offre une synthèse des missions de test du plan selon différents critères :

- Origine
- Priorité
- Catégorie
- Score
- Statut

Charge de travail et ressources

Ce rapport permet de comparer les charges de travail estimées et effectives.

Les diagrammes circulaires permettent de visualiser la répartition entre missions de conception et d'efficacité.

Allocation des ressources

Le graphe affiché dans ce rapport permet de comparer :

- les personnes disponibles
- les personnes nécessaires
- les personnes affectées.

Par défaut, les résultats portent sur l'année en cours mais vous pouvez afficher les résultats sur une période précise.

Rapport de Gantt

Le rapport Gantt présente deux parties :

- Un diagramme de Gantt des missions de test du plan planifiées entre les dates sélectionnées.
- Un diagramme de Gantt de l'occupation des contrôleurs sur des missions de test entre les dates sélectionnées.

Dépenses

Ce rapport permet de visualiser l'ensemble des dépenses liées à un plan ainsi que leur répartition par catégorie de dépenses et par contrôleur.

Il permet au directeur de planifier les missions à venir.

Fermer un plan de test

Une fois que toutes les activités de test sont terminées, le directeur du contrôle interne peut fermer le plan de test.

Cette action a pour effet de fermer tous les tests en cours ou qui n'ont pas été annulés.

Tableau de bord du testing

Votre tableau de bord vous permet d'accéder à un ensemble de widgets et de suivre en temps réel l'avancement de vos missions de test.

Pour personnaliser votre tableau de bord :

1. Dans la barre de navigation, cliquez sur **Tableau de bord**.
2. Cliquez sur **Ajouter**.
   La liste des éléments que vous pouvez afficher sur votre tableau de bord apparaît:
   - widgets généraux
   - widgets relatifs aux problématiques GRC
3. Sélectionnez un élément.
   Celui-ci apparaît dans votre tableau de bord.

GÉRER LES DÉFAILLANCES ET PLANS D'ACTION

Des défaillances sont identifiées à partir de questionnaires d'évaluation des contrôles. Leur analyse permet de mettre en place des actions correctives adéquates sous forme de plans d'action. Le suivi de ces plans d'action est facilité par la production de rapports.

- ✓ Gérer les défaillances
- ✓ Gérer les plans d'action

GÉRER LES DÉFAILLANCES

Créer une défaillance

Vous pouvez créer des défaillances à tout moment, par exemple lorsqu'une activité de testing fait l'objet d'une mauvaise évaluation.

Pour créer une défaillance :

1. Dans la barre de navigation, cliquez sur **Testing > Traitement > Défaillances**.
2. Cliquez sur **Nouveau**.
3. Saisissez un **Nom**.
4. Dans le champ **Catégorie**, spécifiez s'il s'agit d'une défaillance :
   - détectée lors de l'évaluation des contrôles
   - détectée lors du testing
   - générique
5. Spécifiez l'**Impact** : permet d'évaluer l'impact du problème rencontré (faible, moyen, fort, etc.)
6. Saisissez une **Description**.
7. Cliquez sur **OK**.

Définir le périmètre d'une défaillance

Vous pouvez donner des précisions sur le contexte de détection de la défaillance.

Pour définir le périmètre d'une défaillance :

1. Dans les propriétés de la défaillance, dépliez la section **Périmètre de l'évaluation**.
2. Reliez :
   - une activité de test, ou
   - un ou plusieurs contrôles évalués.

Traiter une défaillance

Pour traiter une défaillance, vous pouvez créer un plan d'action directement sur cette défaillance.

Pour plus de détails, voir Gérer les plans d'action.

Suivre les défaillances

Pour visualiser les défaillances traitées / non traitées :

1. Cliquez sur **Testing > Traitement > Défaillances**.
2. Dans la liste déroulante, sélectionnez :
   - "Défaillances traitées" (dont le plan d'action est terminé)
   - "Défaillances non traitées"

GÉRER LES PLANS D'ACTION

Vous pouvez mettre en place des plans d'action pour améliorer un contrôle qui n'a pas été jugé satisfaisant.

Accéder aux plans d'action

Pour accéder à tous les plans d'action :

- Dans la barre de navigation, sélectionnez **Plans d'action**.

Pour accéder aux plans d'action sur lesquels vous devez intervenir :

1. Dans la barre de navigation, sélectionnez **Plans d'action.**
2. Dans la liste déroulante, sélectionnez **Plans d'action à mettre en œuvre**.

   ☛ *Cette liste affiche les plans d'action que vous devez mettre en œuvre ou approuver.*

Créer un plan d'action dans le cadre du testing

Pour créer un plan d'action dans le cadre du testing:

1. Dans la barre de navigation, sélectionnez **Testing > Plans de test**.
2. Ouvrez les propriétés d'une mission de test.
3. A partir de la liste déroulante, sélectionnez **Programme de travail**.
4. Sélectionnez une défaillance et dans sa fenêtre de propriétés, sélectionnez la page **Plans d'action**.
5. Cliquez sur **Nouveau**.
6. Saisissez son nom et cliquez sur **OK**.
   Le plan d'action est créé, ainsi que le workflow associé.

   ☛ *Pour plus de détails sur le workflow des plans d'action, voir Workflows des plans d'action.*

   ☛ *Le plan d'action apparaît également dans le menu **Testing > Traitement > Plans d'action > Plans d'action traitant les défaillances.***

Voir aussi Caractériser le plan d'action.

Caractériser le plan d'action

Pour accéder aux propriétés du plan d'action :

1. Voir Accéder aux plans d'action.
2. Ouvrez les propriétés du plan d'action.

Vue d'ensemble

La page de propriétés **Vue d'ensemble** d'un plan d'action présente :

- les principales informations sous la forme d'une carte d'identification
- les principaux indicateurs de l'avancement.
- le Gantt des actions avec l'historique d'avancement

> ☛ *Ces informations ne sont pas modifiables dans la vue d'ensemble.*

Ci-dessous les indicateurs d'avancement affichés dans le tableau de bord :

- **Avancement** (en pourcentage)

  > ☛ *Correspond à la valeur de la colonne **Pourcentage d'avancement** du dernier état d'avancement (section **Historique de l'avancement**).*

- **Timing**
  - Dans les temps
  - En retard

  > ☛ *Correspond à la valeur de la colonne **Évaluation de l'avancement** du dernier état d'avancement (section **Historique de l'avancement**)*

- **Résultat**
  - Échec
  - Succès
  - Non connu

  > ☛ *Correspond à la valeur saisie dans le champ **Résultat** de la section **Facteurs de succès et résultats**.*

Caractéristiques générales

Vous pouvez spécifier les informations suivantes :

- **Nom** : nom du plan d'action
- **Priorité**: permet d'indiquer un niveau. La priorité peut être :
  - "Basse"
  - "Moyenne"
  - "Elevée"
  - "Critique".
- **Propriétaire** : ce champ est renseigné par défaut par l'utilisateur qui crée le plan d'action.
- **Entité propriétaire** : entité responsable de la mise en œuvre du plan d'action.
- **Approbateur** : utilisateur responsable de la validation du plan d'action quand toutes les actions sont terminées.
- **Niveau organisationnel** : objectif final du plan ; il peut être :
  - "Global"
  - "Local".
- **Origine** : permet de définir le contexte de réalisation du plan d'action :
  - "Audit"
  - "Conformité"
  - "Evénement"
  - "Risque"
  - "RFC"
  - "Autre".
- **Catégorie** : le plan d'action peut par exemple être lié à :
  - la réduction de l'impact des risques
  - la gestion de projet
  - l'amélioration des processus
  - l'amélioration de la performance des contrôles
  - etc.
- **Nature** : permet de définir s'il s'agit d'un plan d'action :
  - Correctif
  - Préventif.
- **Moyens** : description textuelle des moyens nécessaires /souhaités pour l'exécution du plan d'action.
- **Description** : permet d'apporter un complément d'information sur le plan d'action et ses caractéristiques.
- **Calendrier de pilotage** : permet d'envoyer des rappels à la personne responsable d'un plan d'action afin qu'elle renseigne le taux d'avancement de ce plan d'action.

  ☛ *Un calendrier de pilotage pour un rappel mensuel d'avancement est fournir par défaut.*

Responsabilités

L'utilisateur défini comme **Réalisateur** du plan d'action est responsable de la définition des actions à réaliser ainsi que de leur réalisation.

Ce champ est renseigné par l'utilisateur qui crée le plan d'action ou par l'approbateur du plan d'action.

Analyse financière

- **Coût prévu** : estimation du coût du plan d'action
- **Coût prévu (Jour-Homme)** : estimation exprimée en jours.homme de la charge nécessaire à la mise en œuvre du plan d'action

Facteurs de succès et résultats

Dans la section **Facteur clés de succès**, vous pouvez renseigner de manière textuelle des indicateurs de succès qui permettent de juger de la réussite du plan d'action.

Vous pouvez indiquer le **Résultat** du plan d'action :

- Non connu
- Echec
- Succès

Périmètre

Pour positionner un plan d'action dans son environnement, vous pouvez associer des objets à ce plan d'action dans la section **Périmètre**.

Vous pouvez relier des objets des types suivants :

- contrôles
- applications
- risques
- entités
- catégories de processus
- processus
- incidents
- défaillances

Historique de l'avancement

La section **Historique de l'avancement** permet de suivre l'historique des états d'avancement renseignés par le propriétaire du plan d'action.

Voir Renseigner l'avancement d'un plan d'action

Jalons

Les jalons sont des dates clés du plan d'action.

☛ *La date de fin planifiée est obligatoire.*

Pièces jointes

Vous pouvez joindre des documents métier à un plan d'action ou spécifier une URL.

☛ *Pour plus de détails sur l'utilisation des documents métier, voir le guide **Hopex Common Features**.*

Gérer les actions

☛ *Voir aussi : Gérer les plans d'action.*

Le propriétaire du plan d'action doit définir les actions permettant au plan d'action d'aboutir. Il a la possibilité de créer des actions et les affecter.

📖 *Une action est incluse dans un plan d'action et représente une transformation ou un traitement dans une organisation ou un système.*

Accéder aux actions

Pour accéder aux actions d'un plan d'action :

1. Dans l'arbre de navigation, cliquez sur **Plans d'action**.
2. Ouvrez les propriétés du plan d'action qui vous intéresse.
3. Sélectionnez la page **Actions**.

Créer des actions

Pour créer des actions à partir d'un plan d'action :

1. Voir Accéder aux actions.
2. Dans la page **Actions**, cliquez sur **Nouveau**.
3. Sélectionnez un **Propriétaire**.
4. (facultatif) Précisez les jalons qui sont les dates importantes de l'action.
   - **Date de début planifiée**
   - **Date de fin planifiée**
5. Cliquez sur **OK**.

L'action est créée.

Décrire l'enchaînement des actions

Pour spécifier l'enchaînement des actions :

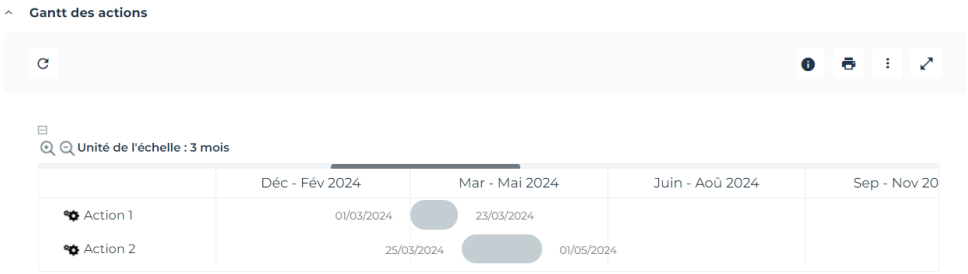
1. Voir Accéder aux actions.
2. Dans la colonne **Suivant**, spécifiez l'action qui suit.

Visualiser le Gantt des actions

Hopex vous permet de visualiser le planning des actions sous forme de diagramme de Gantt.

Pour accéder au diagramme de Gantt des actions :

1. Voir Accéder aux actions.
   Dans la partie inférieure de la page **Actions** des propriétés d'un plan d'action, le Gantt des actions apparaît :



☛ *Vous pouvez également visualiser le Gantt des actions :*

- *dans la page **Rapport d'avancement** des propriétés du plan d'action*
- *dans la page **Vue d'ensemble** des propriétés du plan d'action*

Réassigner des actions

Pour réassigner plusieurs actions :

1. Voir Accéder aux actions.
2. Dans la page **Actions**, sélectionnez les actions concernées.
3. Cliquez sur le bouton **Assignation** qui apparaît.
4. Dans l'assistant proposé, sélectionnez un **Responsable**.
5. Cliquez sur **OK**.

Le responsable initial est remplacé par celui que vous venez de choisir pour toutes les actions concernées.

Workflows des plans d'action

☛ *Voir aussi : Gérer les plans d'action.*

Un workflow est créé automatiquement à la création du plan d'action.

Selon le profil de la personne qui crée le plan d'action, deux workflows sont disponibles :

- approche "top-down"
- approche "bottom-up"

☛ *Les commandes qui permettent de passer d'un statut de workflow à un autre sont disponibles :*

- *dans le menu contextuel du plan d'action à partir d'une liste de plans d'action*
- *dans la fenêtre de propriétés du plan d'action, en cliquant sur l'icône du plan d'action située en haut à gauche*

Approche "bottom-up"

Dans une approche "bottom-up", le plan d'action est créé par un utilisateur quelconque. Un approbateur doit valider le plan d'action pour que celui-ci puisse être mis en oeuvre. C'est le cas lorsque les répondants aux questionnaires d'évaluation des contrôles proposent un plan d'action : ils doivent d'abord le soumettre via le workflow.

☛ *Pour les différentes étapes du workflow, voir Workflow de plan d'action "bottom-up"*

Approche "top-down"

Dans le cadre du workflow "top-down ", le plan d'action est créé par un responsable. Le plan d'action n'a pas besoin d'être validé dans ce cas.

Les contrôleurs internes qui réalisent des missions de testing utilisent cette approche.

☛ *Pour les différentes étapes du workflow, voir Workflow de plan d'action "top-down".*

Workflow des actions

Une fois que les actions d'un plan d'action sont définies, le fait de démarrer le plan d'action démarre les actions liées.

Une fois que le responsable d'action a terminé ses actions, il peut fermer ces dernières. La fermeture du plan d'action ferme automatiquement les actions liées.

☛ *Voir Workflow d'actions*

Renseigner l'avancement d'un plan d'action

☛ *Voir aussi : Gérer les plans d'action.*

Une fois le plan d'action démarré, vous pouvez créer des états d'avancement de manière à rendre compte de son avancement.

Pour renseigner l'avancement du plan d'action :

1. Dans la barre navigation, sélectionnez **Plans d'action > Plans d'action > Plans d'action à mettre en œuvre**.
2. Ouvrez la fenêtre de propriétés d'un plan d'action.
3. Dépliez la section **Avancement du plan d'action** et dans le cadre **Etat d'avancement** cliquez sur **Nouveau**.
4. Spécifiez un **Pourcentage d'avancement**.
5. Donnez éventuellement une **Evaluation de l'avancement**.
   Vous pouvez préciser si le plan d'action est :
   - dans les temps
   - en retard
6. Cliquez sur **OK**.
   L'état d'avancement est créé. Vous pouvez en créer à intervalle régulier.

Rapports de suivi des plans d'action (tableau de bord)

Chemin d'accès

Barre de menu > Rapports

Résultat

Ce rapport est composé de plusieurs graphiques :

- diagrammes en barres
- diagrammes circulaires.

Les plans d'action sont représentés dans leurs différents contextes (processus et entités).

Plans d'action par statut

Ce diagramme en barres présente les statuts des plans d'action.

Plans d'action par avancement

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur statut. Les statuts possibles sont les suivants :

- Dans les temps :
  - en cours
  - avec une date d'échéance supérieure à 30 jours
- En retard :
  - en cours
  - avec une date d'échéance antérieure à la date courante
- Arrivant à échéance :
  - en cours
  - avec une date d'échéance comprise entre 0 et 30 jours
- Annulé
- Fermé

Plans d'action par priorité

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur priorité.

Les priorités possibles sont les suivantes :

- Critique
- Elevée
- Moyenne
- Faible

Plans d'action par catégorie

Ce diagramme circulaire présente le découpage des plans d'action en fonction de leur catégorie.

Les catégories possibles sont les suivantes :

- Correction
- Prévention

Plans d'action par entité

Ce diagramme en barres présente le découpage des plans d'action pour chaque entité.

- En abscisse : toutes les entités
- en ordonnée : nombre de plans d'action liés à chacune des entités et sous-entités

> ☛ *Si aucune entité n'est sélectionnée, toutes les entités racines sont prises par défaut.*

Plans d'action par processus

Ce diagramme en barres présente le découpage des plans d'action pour chaque processus.

- En abscisse : tous les processus (catégories de processus et processus)
- en ordonnée : nombre de plans d'action liés à chacun des processus et ses sous-processus

RAPPORTS CONCERNANT LES CONTRÔLES

Cette section regroupe les principaux rapports utilisés au cours de chaque étape du contrôle interne. Ils peuvent constituer une aide à la décision et vous permettent de suivre l'avancement de vos travaux.

- ✓ Rapport d'environnement d'un contrôle
- ✓ Rapport d'impacts d'un contrôle
- ✓ Rapports du registre des contrôles
- ✓ Rapports d'exécution des contrôles
- ✓ Rapports du testing des contrôles
- ✓ Rapports concernant les défaillances
- ✓ Rapports de conformité informatique et réglementaire

☛ *Pour plus de détails sur les rapports, voir :*

- *Accéder aux rapports*
- *Créer un rapport*

RAPPORT D'ENVIRONNEMENT D'UN CONTRÔLE

Vous pouvez choisir d'afficher les éléments suivants, pour un contrôle donné :

- le contexte du risque
  - catégories de processus
  - processus
  - applications
  - acteurs
  - lignes métier
- les objets stratégiques impactés par le risque (objectifs)
- les conséquences du risque (risques associés)
- les contrôles préventifs visant à remédier au risque

  Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.
- incidents

  Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.
- les plans d'action et actions

Chemin d'accès

Fenêtre de propriétés d'un contrôle (**Rapports > Environnement d'un contrôle**).

Paramètres du rapport

Paramètres	Contraintes
Contrôle	Obligatoire
Contexte du contrôle (catégorie de processus, processus, applications, entités, lignes métier)	Facultatif
Risques traités	Facultatif
Défaillances	Facultatif
Plans d'action	Facultatif
Contexte du risque (catégorie de processus, processus, applications, entités, lignes métier)	Facultatif

Créer un rapport d'environnement de contrôle

Pour afficher le rapport d'environnement d'un contrôle :

1. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Rapports > Environnement d'un contrôle**.
2. Dans la section **Paramètres**, sélectionnez les types d'objets que vous souhaitez afficher :
   - **Contextes du contrôle**
   - **Risques traités**
   - **Défaillances**
   - **Plans d'action**
   - **Contextes du risque**
3. Dans le champ **Affichage du rapport**, indiquez si vous souhaitez afficher les objets de l'environnement du risque de manière :
   - horizontale
   - circulaire (autour du risque sélectionné)
4. Cliquez sur le bouton **Rafraîchir**.

A partir de ce diagramme, vous pouvez :

- replier/déplier des branches
- ouvrir la page de propriétés de l'objet sélectionné

Exemple

RAPPORT D'IMPACTS D'UN CONTRÔLE

Ce rapport est un dendrogramme affichant tous les éléments impactés par un contrôle.

Chemin d'accès

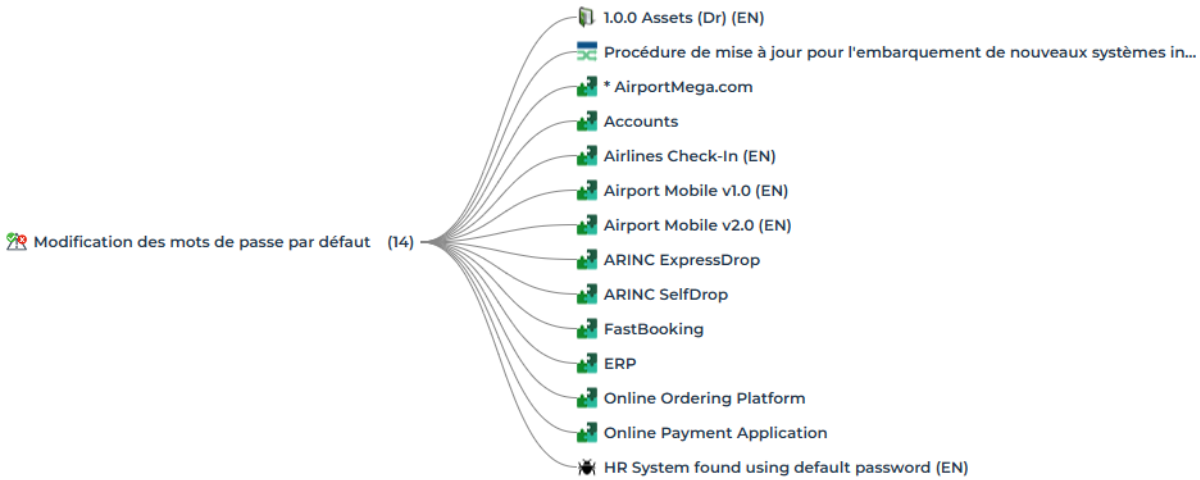
Fenêtre de propriétés d'un risque :

- **Rapports > Impacts d'un contrôle**, ou
- **Vue d'ensemble**

Paramètres du rapport

Paramètres	Type du paramètre
Contrôle	1 contrôle

Exemple



RAPPORTS DU REGISTRE DES CONTRÔLES

Identification des contrôles (tableau de bord)

Ce rapport présente la répartition des contrôles sous plusieurs axes :

- entités
- catégories de processus/processus
- types de contrôle
- comptes

Chemin d'accès

Barre de navigation > Rapports

Paramètres

Paramètres	Remarques
Date de début	Facultatif Tous les contrôles créés après cette date sont sélectionnés.
Date de fin	Obligatoire Initialisé avec la date courante Tous les contrôles créés avant cette date sont sélectionnés.
Objets de contexte	Facultatif L'objet de contexte peut être un(e): - Entité - Type de contrôle - Catégorie de processus/Processus - Compte

Relier des objets de contexte

Vous pouvez spécifier des objets de contexte permettant d'afficher les contrôles liés à des :

- Entités
- Catégories de processus/Processus
- Types de contrôle
- Comptes

Pour relier des objets de contexte :

- Dans le cadre approprié, cliquez sur **Relier** ....
  Dans la fenêtre qui apparaît, vous pouvez sélectionner les objets de deux manières :
  - via une arborescence : sélectionnez les objets à relier dans l'arborescence proposée et cliquez sur **OK**.
  - par l'outil de recherche : sélectionnez le type d'objet désiré dans la liste déroulante, cliquez sur le bouton **Rechercher**, sélectionnez les objets à relier et cliquez sur **OK**.

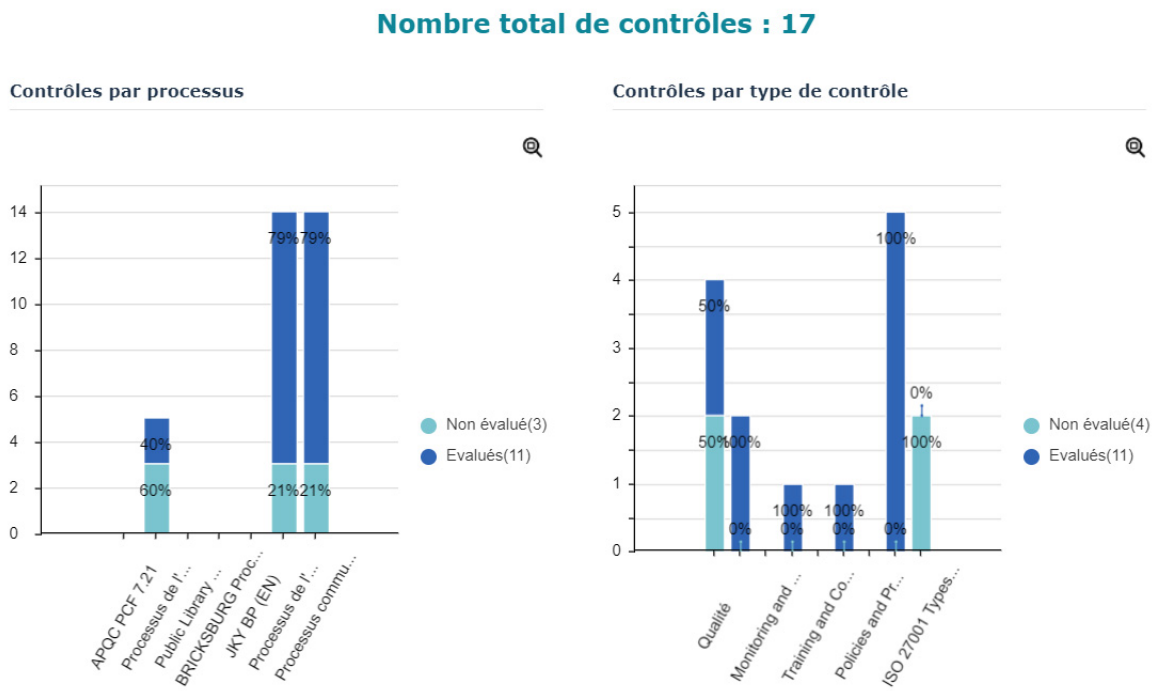
Résultats

Pour obtenir la liste des contrôles qui composent une barre du diagramme :

- Cliquez que la barre du diagramme qui vous intéresse.
  La liste des contrôles pris en compte est présentée en bas de la zone d'édition.

Les barres du diagramme permettent de distinguer les contrôles évalués de ceux qui n'ont pas encore été évalués.

Exemple



RAPPORTS D'EXÉCUTION DES CONTRÔLES

Résultats d'exécution consolidés

Ce rapport présente les résultats agrégés des contrôles par entité et par mois.

Chemin d'accès

Barre de navigaton > Rapports

Paramètres

Paramètres
Calendrier
Date de début
Date de fin
Type d'entité
Entité

Résultat

La matrice est composée :

- d'une liste d'entités : par défaut, toutes les entités sont sélectionnées.

  ☛ *Si le paramètre "Type d'entité" est renseigné, les entités sélectionnées correspondent au type d'entité spécifié.*

- du **Nombre total de contrôles** : nombre de contrôles liés à l'entité (ou à ses sous-entités).
- du **Nombre total d'instances** : les contrôles sont comptés autant de fois qu'il y a de contextes pour un même contrôle.

  Si un contrôle est évalué dans le cadre de deux entités différentes, le contrôle est compté deux fois : **Hopex**

Internal Control distingue deux instances de contrôle évalué.

☛ *Pour plus de détails sur la contextualisation des contrôles, voir Contextualiser les contrôles.*

- pour chaque mois :
  - du **Nombre d'instances évaluées**
  - du nombre d'instances qui se sont révélées satisfaisantes
  - du % d'instances qui se sont révélées satisfaisantes

Exemple

Q1 2016 - Consolidation par entités

			Jan-2016			Fév-2016		
	Nombre total de contrôles	Nombre total d'instances	Nombre d'instances évaluées	Nombre d'instances OK	% Instances OK	Nombre d'instances évaluées	Nombre d'instances OK	% Instances OK
Belgique	9	9	0	0	0 %	8	0	0 %
Etats-Unis	11	11	0	0	0 %	12	0	0 %
France	16	18	0	0	0 %	12	0	0 %
Italie	9	9	0	0	0 %	10	0	0 %
Japon	3	3	0	0	0 %	0	0	0 %

Suivi des sessions d'exécution

Ce rapport permet de suivre les sessions d'évaluation de type "Exécution".

Chemin d'accès

Ce rapport est disponible depuis une session d'exécution.

Pour accéder à ce rapport depuis une session d'exécution :

1. Dans la page de propriétés d'une campagne d'exécution, sélectionnez la page **Sessions** et ouvrez la page de propriétés d'une session.
2. Sélectionnez la page **Suivi**.

Paramètres

Paramètres
Session

Résultat

Un résumé affiche des informations générales sur la session d'exécution courante.

Ce rapport présente plusieurs graphiques concernant l'avancement de la session d'exécution :

- Pourcentage des questionnaires remplis
- Pourcentage de questionnaires validés
- Répartition des questionnaires par statut, pour chaque répondant

RAPPORTS DU TESTING DES CONTRÔLES

Couverture des missions de test

Le rapport de couverture des missions de test constitue une aide à la décision lors de la sélection des missions de test.

Il permet de générer des missions de test.

☛ *Voir Visualiser le rapport de couverture des missions de test*

Synthèse d'un plan

Ce rapport présente une vue d'ensemble des indicateurs d'un plan.

Chemin d'accès

Propriétés d'un plan > Rapports > Supervision

Résultat

Un tableau de synthèse présente :

- le nombre de missions (nombre total, nombre de missions planifiées, publiées et terminées)

  ☛ *Si vous cliquez sur le chiffre indiqué, les missions correspondantes apparaissent en bas de la fenêtre. Vous pouvez consulter les propriétés de chaque mission de test et les modifier à partir de cette liste.*
- la charge de travail estimée et effective (en jours)
- la durée moyenne (en jours)
- le nombre moyens de contrôleurs

Des graphes présentent la répartition des missions de test par :

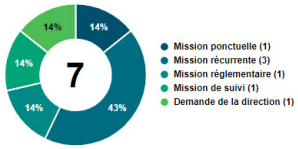
- origine
- priorité
- catégorie
- score
- statut

Exemple

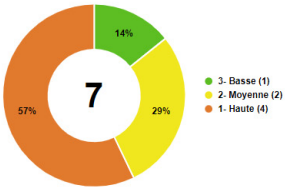
Tableau de synthèse

Toutes	Planifiées	Publiées	Terminées	Charge de travail estimée (Jours)	Charge de travail effective (Jours)	Durée moyenne (Jours)	Nombre moyen d'auditeurs
7	7	7	6	0	110	0	2.2

Par origine



Par priorité



Autres rapports

Des rapports vous permettent de suivre l'avancement d'un objet en particulier (plan de test, mission de test, plan d'action). Il sont disponibles sur chaque objet, dans le menu **Testing** de la barre de navigation.

Rapports de suivi d'un plan de test

Des rapports permettent de suivre l'exécution d'un plan de test.

☛ *Voir Afficher les rapports de suivi d'un plan de test.*

Rapport de suivi d'une mission de test

Pour plus d'informations sur les possibilités offertes pour le suivi d'une mission de test en particulier, voir :

- Planifier les missions de test via un diagramme de Gantt
- Visualiser la disponibilité des ressources
- Consulter le rapport du programme de travail
- Générer le rapport de la mission de test
- Rapports des dépenses d'une mission de test
- Superviser la mission de test
- Rapports d'évaluation de la mission de test

Rapport d'un plan d'action

Pour suivre l'avancement d'un plan d'action en particulier, voir Suivre l'avancement d'un plan d'action.

RAPPORTS CONCERNANT LES DÉFAILLANCES

Défaillances par statut de traitement

Le rapport de suivi des défaillances se présente sous forme d'un diagramme circulaire.

Chemin d'accès

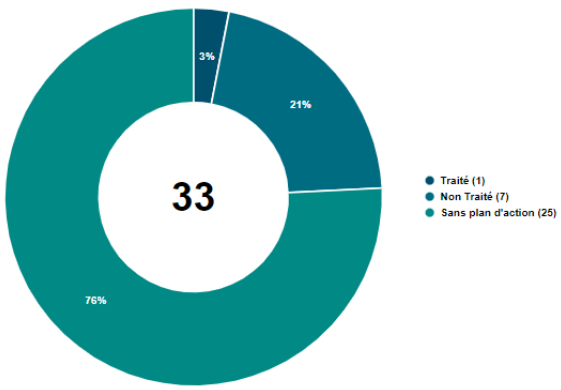
Barre de navigation > Rapports

Résultat

Ce rapport permet de distinguer les défaillances :

- **Traitées** : défaillances ayant un plan d'action dont le statut est :
  - "Terminé"
  - "Fermé"
- **Non traitées** : défaillances ayant un plan d'action dont le statut est :
  - "A envoyer"
  - "A démarrer"
  - "En cours"
- **Sans plan d'action**

Exemple



Défaillances par impact

Ce rapport est un diagramme circulaire qui regroupe les défaillances par impact (très faible, moyen, fort, très fort).

Vous pouvez filtrer les résultats :

- par statut de défaillance (ouvert, fermé)
- par type de contrôle impacté par la défaillance.

Cas d'utilisation exemple :

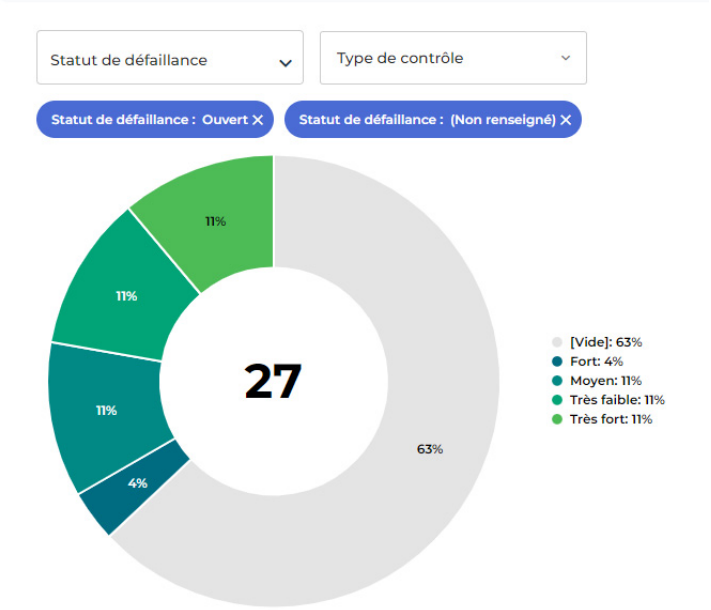
- vous avez relié un certain nombre de contrôles à un type de contrôle pour répondre à des exigences spécifiques (par exemple, "Conformité informatique")

- ce rapport vous permet de visualiser les seules défaillances qui impactent le type de contrôle en question.

Chemin d'accès

Barre de navigation > Rapports

Résultat



HOPEX Enterprise Risk Management

Guide d'utilisation

HOPEX Aquila 6.2

Bizzdesign

SOMMAIRE

Sommaire

GÉRER LES RISQUES

Pour maîtriser les risques, il est nécessaire d'identifier et de qualifier les risques encourus dans le déroulement d'un processus.

> 🕮 *Un risque est un danger plus ou moins probable auquel est exposée une organisation.*

Une fois les risques analysés et évalués, le management détermine quels traitements appliquer à chacun de ces risques. **Hopex Enterprise Risk Management** offre des outils qui facilitent la création et l'analyse des risques afin d'identifier les risques les plus importants et de mettre en place les actions correctives ou préventives adaptées.

Les points suivants sont abordés ici :

- ✓ Profils de connexion de gestion des risques
- ✓ Créer un risque
- ✓ Caractéristiques d'un risque
- ✓ Accéder aux risques
- ✓ Workflow des risques

PROFILS DE CONNEXION DE GESTION DES RISQUES

Pour se connecter à Hopex, voir **Hopex Common Features**, "Le bureau Hopex", "Accéder à Hopex (Web Front-End)".

Profils	Tâches
Risk Manager (ou Manager GRC)	Responsable de l'exécution des tâches suivantes concernant les risques de son domaine de responsabilité : - identifier les risques - réaliser des évaluations directes - gérer les campagnes d'évaluation - définir des plans d'action - analyser et suivre la création de rapports
Contributeur GRC	- Répond aux questionnaires d'évaluation - Définit et élabore les plans d'action Voir Bureau des contributeurs GRC.

☛ *Pour plus de détails, voir également Accéder au bureau GRC.*

CRÉER UN RISQUE

Pour créer un risque :

1. Dans la barre de navigation, sélectionnez **Risques**.
2. Cliquez sur **Nouveau**.

   ☛ *Vous pouvez également créer un risque depuis la page d'accueil (zone d'**Accès rapide > Actions > Créer un risque**).*
3. Saisissez un **Nom**
4. (optionnel) Spécifiez le **Mode d'identification du risque**
   Le risque peut avoir été identifié à partir, par exemple :
   - d'une "base d'incidents"
   - d'un "atelier"
   - d'un "sondage"
   - d'une "mission d'audit"
5. (optionnel) Saisissez une **Description**
6. Cliquez sur **OK**.

Vous pouvez compléter la description du risque via sa fenêtre de propriétés.

Voir :

- Caractéristiques d'un risque
- Workflow des risques

CARACTÉRISTIQUES D'UN RISQUE

☛ *Pour accéder aux risques, voir Accéder aux risques.*

☛ *Pour pouvoir évaluer des risques dans le cadre de campagnes d'évaluation par questionnaires, vous devez avoir renseigné certaines propriétés. Pour plus de détails, voir Préparer l'environnement de l'évaluation.*

Caractéristiques générales

Pour accéder aux caractéristiques d'un risque :

❱ Cliquez sur un risque dans la liste de risques.

Dans la page de propriétés, vous pouvez préciser :

- le **Code** d'identification du risque
- que le risque est de haut niveau en cochant la case **Risque majeur**
- le **Propriétaire** du risque
- le **Mode d'identification** du risque
  Le risque peut avoir été identifié à partir, par exemple :
  - d'une "base d'incidents"
  - d'un "atelier"
  - d'un "sondage"
  - d'une "mission d'audit"
- la **Description détaillée** du risque

☛ *le **Statut** du risque n'est pas modifiable parce qu'il est géré par le workflow associé au risque.*

Voir aussi :

- Analyser un risque
- Responsabilités (RACI) sur risque
- Vue d'ensemble d'un risque
- Définir le périmètre d'un risque (définition du périmètre du risque)

Vue d'ensemble d'un risque

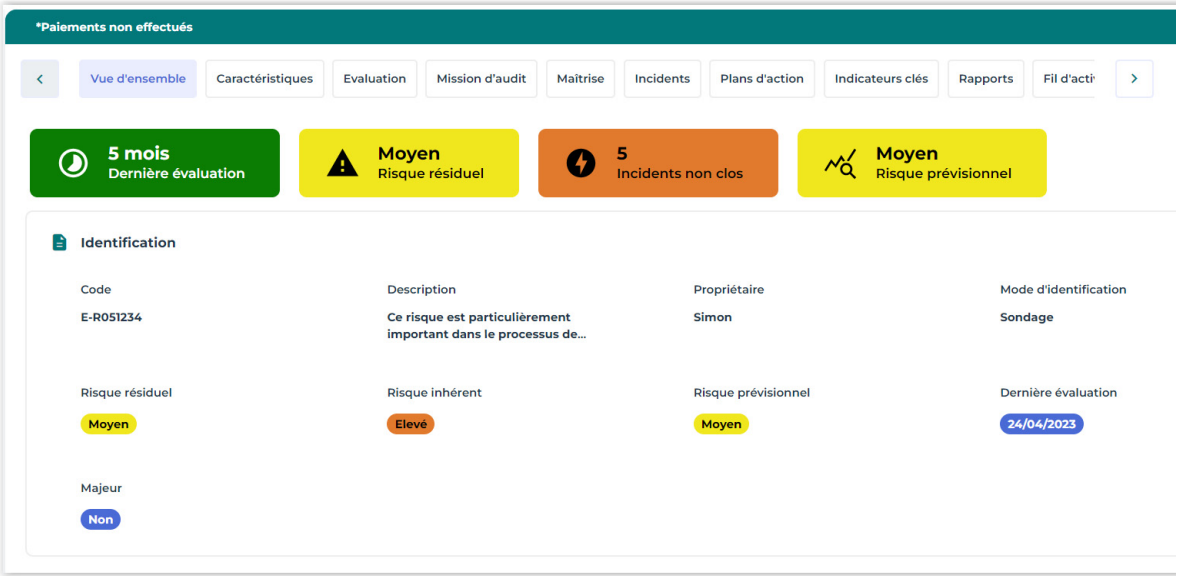
☛ *Pour accéder aux risques, voir Accéder aux risques.*

La page de propriétés **Vue d'ensemble** donne accès à:

- une carte du risque, qui fournit un aperçu des principales caractéristiques du risque.

  ☛ *Pour plus de détails sur les cartes d'objets, voir Carte d'un objet, dans la section "Plateforme - Fonctionnalités communes".*

- des informations calculées, sous forme de tableau de bord



Voici les informations calculées fournies dans ce tableau de bord :

- **Dernière évaluation**: temps (en nombre de mois) qui s'est écoulé depuis la dernière évaluation (directe ou par campagne)

  ☛ *Cet indicateur permet de se rendre compte si le risque est évalué de manière régulière. Il peut être utile pour décider de quand réaliser la prochaine évaluation.*

- **Risque résiduel** : moyenne du risque net obtenu à partir de la dernière session d'évaluation. Tous les contextes pour lesquels le risque a été évalué sont pris en compte (entités, processus, application).

  📖 *Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.*

- **Incidents non clos** : nombre d'incidents matérialisant le risque et qui se trouvent dans un statut de workflow autre que "Fermé".

  ☛ *Voir Collecte des incidents pour plus de détails sur les incidents.*

- **Risque prévisionnel** : représente la projection du risque net sur l'année à venir (moyenne du risque net).

Responsabilités (RACI) sur risque

☛ *Pour accéder aux risques, voir Accéder aux risques.*

La page de propriétés d'un risque présente une section **Responsabilités** pour définir les différentes personnes responsables de la gestion de ce risque. Pour plus de détails, voir Les responsabilités (RACI).

Notez que le Correspondant Risque, qui répond aux questionnaires concernant les risques, est à spécifier dans les propriétés des objets de contexte reliés aux risques (entités/processus/applications).

☛ *Pour plus de détails, voir :*

- *Pré-requis à l'évaluation des risques*
- *Spécifier les responsabilités au sein d'une entité.*

Voir aussi :

- Définir le périmètre d'un risque
- Analyser un risque
- Vue d'ensemble d'un risque

Définir le périmètre d'un risque

Contextualiser un risque consiste à définir son périmètre.

Pour définir le périmètre d'un risque :

❱ Dans la fenêtre de propriétés d'un risque, dépliez la section **Périmètre**.

Le périmètre peut être constitué de différents types d'objets :

- les **Catégories de processus** et **Processus** exposés au risque. Voir Gérer les catégories de processus et processus.

  🕮 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

  🕮 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

- les **Opérations**

  🕮 *Une opération est une étape élémentaire d'un processus. Elle correspond à l'intervention d'un acteur de l'organisation.*

- les **Entités** concernées par le risque. Voir Gérer les entités.

  🕮 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité*

externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.

☛ *Définir les entités d'un risque constitue une étape préliminaire à l'évaluation des risques. Voir aussi Préparer l'environnement de l'évaluation.*

- les **Objectifs** attendus vis à vis de la gestion du risque.

  🕮 *Un objectif est un but que l'on cherche à atteindre ou la cible visée pour un processus ou une opération. Il permet de mettre en évidence les points que l'on veut améliorer pour ce processus ou cette opération.*

- les **Applications** : Voir Gérer les applications.

  🕮 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

- les **Lignes métier** : Voir Gérer les lignes métier.

  🕮 *Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.*

Analyser un risque

L'analyse d'un risque a pour objectif d'obtenir une bonne compréhension de ce risque. Il s'agit de prendre en compte :

- les causes du risque,
- les conséquences positives ou négatives de ce risque.

La phase d'analyse permet d'associer un risque à :

- des types de risque
- des facteurs de risques
- des conséquences
- d'autres risques

Pour analyser un risque :

1. Voir Accéder aux risques.
2. Sélectionnez un risque et ouvrez sa page de propriétés.
3. Sous l'onglet **Caractéristiques**, dépliez la section **Analyse**.
   Un risque est caractérisé par :
   - des **Types de risque**, pour plus de détails, voir Les types de risque.

     🕮 *Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.*

   - des **Facteurs de risque**, pour plus de détails, voir Les facteurs de risque.

     🕮 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté*

technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.

- des **Conséquences de risque** : pour plus de détails, voir Les conséquences des risques.

  📖 *Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.*

- des **Risques associés**

  ☛ *Les incidents reliés au risque apparaissent dans la page **Incidents** des propriétés du risque*

Les types de risque

Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.

Un type de risque permet de caractériser un risque. Un risque peut par exemple être de type réglementaire, juridique, technique, etc.

Pour créer vos propres types de risque :

1. Dans la barre de navigation, cliquez sur **Risques > Par types de risque**.
2. Cliquez sur **Nouveau**.
3. Renseignez le nom du type de risque et cliquez sur **OK**.
   Le nouveau type de risque apparaît dans l'arborescence du navigateur.

   ☛ *Vous pouvez de la même manière créer un sous-type de risque à partir d'un type de risque.*

Les facteurs de risque

Beaucoup de facteurs de risque sont définis dans le cadre de réglementations internationales, nationales ou inter-professionnelles, ou au sein de l'entreprise elle-même.

📖 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.*

Il est possible d'associer à chaque risque un ou plusieurs facteurs de risque, sources de risques ou dangers qui ont intrinsèquement le potentiel de mettre en danger le fonctionnement de l'organisation. Par exemple, des produits chimiques dangereux, des concurrents, des gouvernements, etc.

Les conséquences des risques

Pour définir les conséquences associées à un risque :

1. Voir Accéder aux risques.
2. Dans les propriétés d'un risque, section **Analyse**, onglet **Conséquences de risque**, cliquez sur l'onglet **Nouveau**.

La conséquence créée apparaît dans la liste des conséquences associées au risque.

Visualiser les recommandations d'audit liées à un risque

Pour visualiser les recommandations liées à un risque :

1. Voir Accéder aux risques.
2. Dans les propriétés d'un risque, sélectionnez la page **Missions d'audit**.

> ☛ *Cette page est disponible si :*
>
> - *vous disposez de **Hopex Internal Audit**.*
> - *vous avez pour profil "Directeur de l'audit" ou "Administrateur fonctionnel GRC".*

Cette page contient :

- les recommandations ayant le risque dans leur périmètre
- les recommandations reliées à un constat ayant le risque dans son périmètre

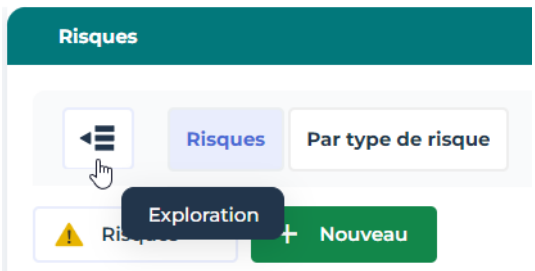
Pour plus de détails sur les risques et recommandations dans le cadre d'une mission d'audit, voir :

- Définir et évaluer les risques découverts lors de la mission d'audit
- Émettre des recommandations

Explorer l'environnement d'un risque

Pour explorer les objets de l'environnement d'un risque :

1. Voir Accéder aux risques.
2. Dans la liste des risques, cliquez sur le bouton **Exploration**.



Des cartes apparaissent pour chaque risque.

3. Passez la souris sur une carte et cliquez sur **Environnement**.

Les éléments de l'environnement du risque s'affichent dans des arborescences. Il s'agit du périmètre étendu du risque.

- **Éléments en risque** (par exemple, processus)
- Éléments de **Maîtrise** (contrôles)
- **Plans d'action en cours**


*Mauvaises entrées des paramètres du contrat...
Soumis
Code: P-R13
Résiduel: Moyen
Appétence: Elevé
Dernière évaluation: 21/09/2022
Majeur: Non
Élément en risque
Processus
Contractualisation
Maîtrise
*Contrôle sur les paiements
Plan d'action en cours
Bilan annuel des contrats fourn

ACCÉDER AUX RISQUES

Accéder à tous les risques

Pour accéder aux risques :

- Dans la barre de navigation, Sélectionnez **Risques.**

Pour chaque risque, vous pouvez visualiser les informations suivantes :

- **Code**
- **Statut**

  ☛ *Le **Statut** permet de distinguer les risques qui ont été **Soumis** (et qui méritent d'être examinés) de ceux qui ont déjà été **Validés**.*
- **Risque majeur** (s'agit-il d'un risque majeur ou non)
- **Entités**
- **Dernière évaluation** (date)
- **Risque inhérent**

  🕮 *Le risque inhérent (ou risque brut) est le risque auquel une entité est exposée en l'absence de mesures correctives par le management pour en modifier la probabilité d'occurrence ou l'impact, par opposition au risque résiduel.*
- **Risque résiduel**

  🕮 *Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.*
- **Incidents non clos** (en nombre)
- **Risques prévisionnels** (en nombre)
- **Plans d'action** (en nombre)

Accéder aux risques par type de risque

Pour accéder aux risques par type de risque :

- Dans la barre de navigation, cliquez sur **Risques > Par type de risque**.

Cette liste affiche tous les risques de votre environnement dans une arborescence structurée autour des types de risque.

Des colonnes affichent, pour chaque type de risque, le nombre de **Risques**.

Pour chaque risque, les informations suivantes son affichées en colonne :

- **Entités** reliées
- **Dernière évaluation**
- **Risque résiduel**

  Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.

- **Risque prévisionnel**

  Le risque prévisionnel représente la projection du risque résiduel sur l'année à venir.

  D'autres colonnes sont disponibles mais non affichées par défaut. Vous pouvez les rajouter.

Accéder aux risques orphelins

Pour accéder aux risques qui ne sont reliés à aucun contexte (risques orphelins) :

1. Voir Accéder à tous les risques.
2. A partir de la liste déroulante **Risques**, sélectionnez **Risques orphelins.**

Cette liste affiche tous les risques qui n'ont pas d'impact connu sur l'organisation. Ces risques ne sont reliés à aucun/e processus, application, entité ou ligne métier.

*Pour spécifier l'impact d'un risque, remplissez la section **Périmètre** des caractéristiques du risque.*

Accéder aux risques matérialisés

Un risque qui s'est matérialisé est un risque pour lequel un incident s'est produit.

Pour accéder aux risques qui se sont matérialisés par un incident :

1. Voir Accéder à tous les risques.
2. A partir de la liste déroulante **Risques**, sélectionnez **Risques matérialisés.**

WORKFLOW DES RISQUES

Le processus de création d'un risque est géré par un workflow. Seuls certains profils sont autorisés à créer, soumettre, valider ou rejeter un risque.

> ☛ *Pour plus de détails sur le workflow de création d'un risque, voir Workflows liés aux risques.*

Etapes de validation d'un risque

Les étapes du processus de validation d'un nouveau risque sont les suivantes :

- Après avoir renseigné les caractéristiques d'un nouveau risque, le créateur d'un risque (qui en est aussi propriétaire) doit **Soumettre** le risque.
- Quand un risque a été soumis, le Risk Manager peut :
  - **Valider** le risque (il prend le statut "Validé").
    Une notification est envoyée par mail à l'utilisateur Propriétaire.
  - **Rejeter** le risque.
    Dans ce cas, le risque prend le statut "Rejeté", mais il n'est pas supprimé.

Valider ou rejeter un risque

Pour valider ou rejeter un risque :

1. Voir Accéder à tous les risques.
2. A partir de la liste déroulante **Risques**, sélectionnez **Risques à examiner**.
3. Sélectionnez le risque et utilisez le bouton **Workflow** pour le valider ou le rejeter.

> ☛ *Vous pouvez également sélectionner plusieurs risques pour effectuer une transition en masse.*

ÉVALUER LES RISQUES

Après avoir identifié et analysé les risques encourus par l'entreprise, il est essentiel de mettre en évidence les risques les plus importants afin de les traiter.

Dans **Hopex Enterprise Risk Management**, l'estimation des risques est qualitative : l'impact d'un risque est décrit par des termes qui correspondent à une échelle prédéfinie (par exemple de 1 à 4). Une cartographie des risques peut ainsi être établie afin d'identifier rapidement les risques les plus critiques.

- ✓ Types d'évaluation des risques
- ✓ Pré-requis à l'évaluation des risques
- ✓ Évaluation directe des risques
- ✓ Visualiser et analyser les résultats d'évaluation de risque

TYPES D'ÉVALUATION DES RISQUES

Une évaluation de risques est destinée à donner des valeurs, dans un contexte précis, à des caractéristiques telles que :

- l'impact
- la probabilité
- le niveau du dispositif de maîtrise du risque

Évaluation directe ou par campagne

Les risques peuvent être évalués :

- unitairement, dans les propriétés d'un risque : voir Créer une évaluation directe sur un risque.
- simultanément, via une (cartographie) interactive : voir Évaluer plusieurs risques simultanément.
- via un questionnaire d'évaluation envoyé à des destinataires appropriés : voir Lancer une campagne d'évaluation.

> ☛ *Les questionnaires envoyés via les campagnes se présentent sous forme de cartographie (heatmap).*

Les résultats de l'évaluation des risques peuvent être présentés dans des rapports dédiés qui facilitent l'analyse des risques évalués. Pour plus de détails, voir Rapports concernant les risques.

> ☛ *Voir aussi : Pré-requis à l'évaluation des risques.*

Modèles d'évaluation pour les risques

Hopex propose deux perspectives différentes pour évaluer les risques :

- Evaluation des risques par entité et processus
- Evaluation des risques par application

> ☛ *Voir aussi : Pré-requis à l'évaluation des risques.*

PRÉ-REQUIS À L'ÉVALUATION DES RISQUES

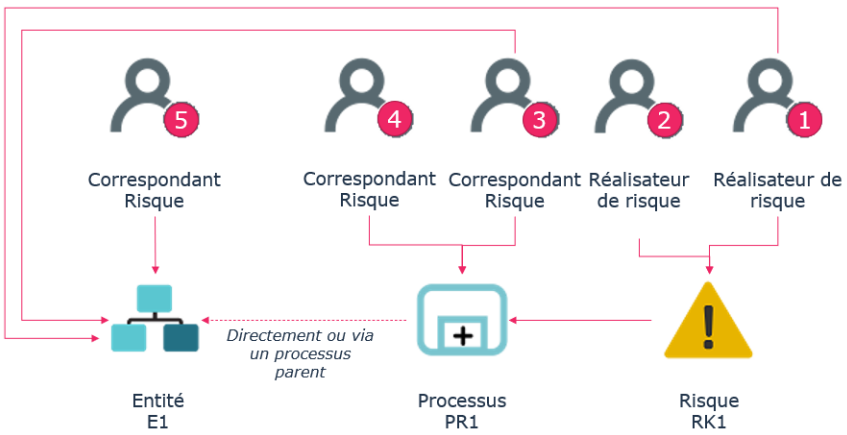
Modèle "Évaluation des risques par entité et processus"

Avant de lancer une campagne d'évaluation de risques, assurez-vous d'avoir :

- relié les risques à au moins une entité/un processus
- spécifié un ou plusieurs répondants dans la fenêtre de propriétés de l'entité/du processus (Correspondant Risque)

Les répondants aux questionnaires de risque peuvent être définis sur :

- des entités
- des processus reliés aux entités (directement ou via un processus parent)
- des risques reliés aux processus (directement ou via un risque)



Logique de définition des répondants

Modèle "Évaluation des risques par application"

Avant de lancer une campagne d'évaluation de risques, assurez-vous d'avoir :

- relié les risques à au moins une application
- spécifié un ou plusieurs répondants dans la fenêtre de propriétés de l'application (Propriétaire de l'application)

ÉVALUATION DIRECTE DES RISQUES

L'évaluation directe permet de fournir, à une date donnée, une évaluation d'un risque sur une entité de l'organisation.

Dans le cadre de l'évaluation directe, les valeurs des caractéristiques peuvent être spécifiées de deux façons :

- dans les propriétés de chaque risque : Créer une évaluation directe sur un risque
- globalement, via une cartographie (heatmap): Évaluer plusieurs risques simultanément

L'évaluation directe est effectuée pour tous les acteurs ou applications disponibles dans la section **Périmètre** de la fenêtre de propriétés du risque.

☛ *Voir aussi : Lancer une campagne d'évaluation.*

Modèles d'évaluation directe des risques

Hopex Enterprise Risk Management propose des modèles d'évaluation des risques dans le contexte des types d'objets suivants :

- entité et processus
- application

Les caractéristiques évaluées

🕮 *Une caractéristique évaluée définit ce que l'évaluation cherche à évaluer. Elle peut être associée à une MetaClasse et précisément à l'un de ses MetaAttributs, par exemple : Metaclasse Risque, MetaAttribut: Criticité.*

Exemple de caractéristiques évaluées :

- Impact
- Probabilité
- Dispositif de maîtrise du risque

  🕮 *Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.*
- Risque résiduel

  🕮 *Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.*

Les répondants

Les répondants sont les personnes définies comme :

- ***Réalisateur de risque*** (sur le risque), ou comme
- ***Correspondant Risque*** (sur l'entité ou un processus).

> ☛ *Il est possible de définir plusieurs répondants.*
>
> ☛ *Pour plus de détails, voir Pré-requis à l'évaluation des risques.*

Le questionnaire

Le questionnaire porte sur les caractéristiques à évaluer pour l'ensemble des risques faisant l'objet d'une évaluation :

- Impact
- Probabilité
- Dispositif de maîtrise du risque

> 🕮 *Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.*

Créer une évaluation directe sur un risque

Vous pouvez créer de nouvelles évaluations en vue d'évaluer un risque sur l'ensemble des objets de l'organisation auxquels il est relié.

Il s'agit d'une évaluation à dire d'expert.

Pour créer une évaluation directe sur un risque :

1. Sélectionnez le risque et ouvrez sa page de propriétés.
2. Sélectionnez la page **Evaluation**.
3. Cliquez sur **Nouvelle évaluation**.

   > ☛ *Une fenêtre proposant de sélectionner le(s) contexte(s) apparaît si plusieurs contextes sont possibles pour le risque concerné.*

4. Donnez les valeurs des caractéristiques pour le risque évalué :
   - **Impact** : impact du risque lorsqu'il se manifeste
   - **Probabilité** : probabilité que le risque se manifeste

     > ☛ *Si le risque a déjà été évalué, les valeurs de l'impact et de la probabilité issues de la dernière évaluation sont proposées par défaut. Vous pouvez modifier ces valeurs pour cette nouvelle évaluation.*

   - **Dispositif de maîtrise du risque**

     > 🕮 *Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.*
     >
     > ☛ *Si le risque a déjà été évalué, une valeur est également proposée pour le niveau du dispositif de maîtrise du risque. Pour plus de détails sur la méthode de calcul, voir Dispositif de maîtrise du risque (DMR).*

5. Spécifiez le cas échéant la **Date d'évaluation**.
6. Cliquez sur **OK**.
   Une évaluation est créée.

Évaluer plusieurs risques simultanément

Vous pouvez évaluer plusieurs risques simultanément via une ***cartographie (heatmap) interactive***.

Pour évaluer simultanément plusieurs risques :

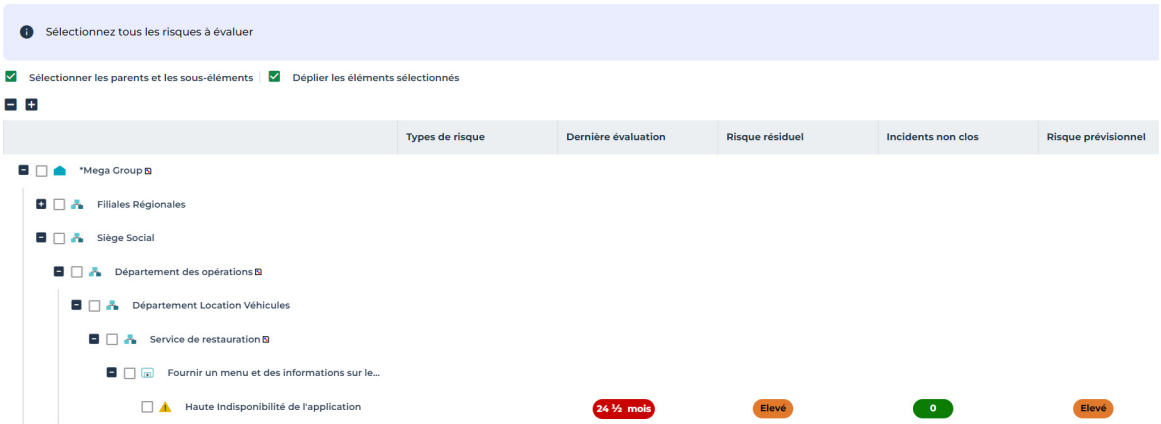
1. Dans la barre de navigation, cliquez sur **Évaluation > Évaluation directe > Évaluation multiple des risques**.
2. Cliquez sur **Nouvelle évaluation**.
3. Dans la fenêtre qui apparaît, sélectionnez le **Modèle d'évaluation** :
   - **Évaluation des risques par entité et processus**
   - **Évaluation des risques par application**
4. Dans l'arborescence affichée, sélectionnez les objets qui définissent le contexte de l'évaluation (entité ou application selon le modèle sélectionné).

   ☛ *Un risque est évalué dans le contexte des éléments de la branche qui remonte du risque jusqu'à la racine.*

   Pour vous faciliter le choix des risques à évaluer, des informations concernant le risque apparaissent en colonne :

   - **Types de risque**
   - **Dernière évaluation**
   - **Risque résiduel**
   - **Incidents non clos**
   - **Risque prévisionnel**

   ☛ *Ces informations sont par ailleurs disponibles dans le tableau de bord du risque. Pour plus de détails, voir Vue d'ensemble d'un risque.*



Dans l'exemple ci-dessus, si vous avez sélectionné l'entité "Département des opérations", sont sélectionnés :
- tous les risques et objets contextes d'un niveau inférieur

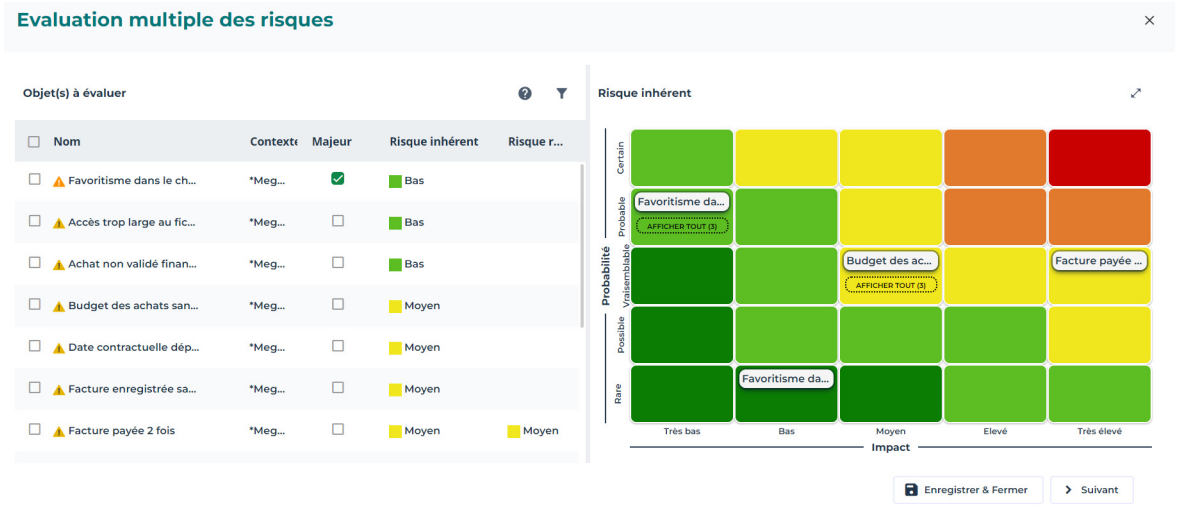
- tous les objets contextes parents jusqu'à la racine de l'arborescence.

> ☛ *Si vous dé-sélectionnez un nœud d'une branche, seuls les enfants de cette branche sont dé-sélectionnés.*

> ☛ *Si des évaluations ont déjà été effectuées, les valeurs de l'évaluation la plus récente sont présentées en colonne.*

5. Cliquez sur **Suivant**.
   Un récapitulatif de l'évaluation apparaît, vous permettant ainsi d'avoir une **Vue d'ensemble** des objets que vous allez évaluer.
6. Cliquez sur **OK**.
   Une cartographie (heatmap) apparaît. Elle permet d'évaluer les risques de manière visuelle.
7. (premier écran) Positionnez les risques sur la cartographie de manière à spécifier :
   - verticalement, l'**Impact** (de rare à certain)
   - horizontalement, la **Probabilité** (de très basse à très élevée)

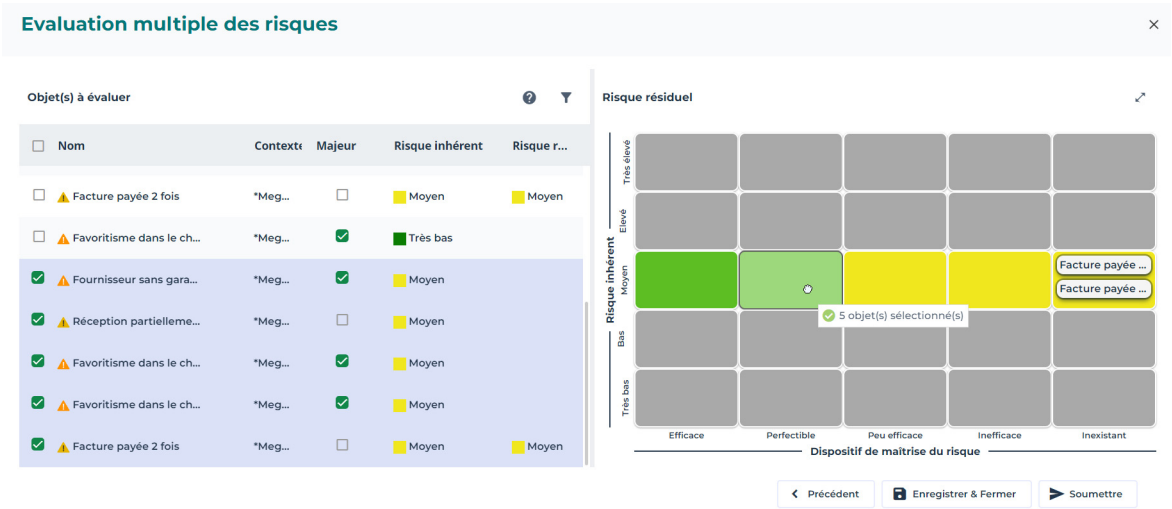
> ☛ *Les valeurs saisies lors de la dernière évaluation s'affichent par défaut.*



8. Cliquez sur **Suivant**.

9. Spécifiez horizontalement le niveau du **Dispositif de Maîtrise du Risque** (d'efficace à inexistant).

> ☛ *Verticalement, vous retrouvez ici le **Risque inhérent**, calculé à partir des données de l'écran précédent.*



10. Une fois que vous avez terminé, cliquez sur **Soumettre**.

Vous pouvez également choisir d'**Enregistrer & Fermer** le questionnaire pour reprendre l'évaluation plus tard. Dans ce cas, le questionnaire est enregistré dans la liste **Évaluations directes en cours**.

> ☛ *Pour plus de détails, voir Utiliser les questionnaires de type heatmap (cartographie), dans la section Fonctionnalités communes.*

Soumettre a pour effet de créer une évaluation dans la page **Évaluation** de la fenêtre de propriétés d'un risque. Pour plus de détails, voir Afficher les résultats d'une évaluation de risque.

VISUALISER ET ANALYSER LES RÉSULTATS D'ÉVALUATION DE RISQUE

Afficher les résultats d'une évaluation de risque

Pour afficher les résultats d'évaluations réalisées sur un risque :

1. Dans la liste des risques, sélectionnez la page **Evaluation** des propriétés du risque.
2. (optionnel) Sélectionnez l'élément de contexte et le modèle qui vous intéressent et cliquez sur **Appliquer les filtres**.
   Les évaluations correspondantes s'affichent. Vous pouvez ainsi filtrer lorsque de nombreuses évaluations ont été réalisées.

> ☛ *Seul l'administrateur fonctionnel GRC peut supprimer les résultats de l'évaluation (c'est-à-dire les nœuds d'évaluation).*
>
> *Pour supprimer un nœud d'évaluation, sélectionnez-le et cliquez sur **Supprimer**.*

Pour chaque nœud d'évaluation les valeurs suivantes sont calculées :

- le risque inhérent

> 🕮 *Le risque inhérent (ou risque brut) est le risque auquel une entité est exposée en l'absence de mesures correctives par le management pour en modifier la probabilité d'occurrence ou l'impact, par opposition au risque résiduel.*

- le risque résiduel

> 🕮 *Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.*

Générer des rapports sur les évaluations

Rapports instantanés

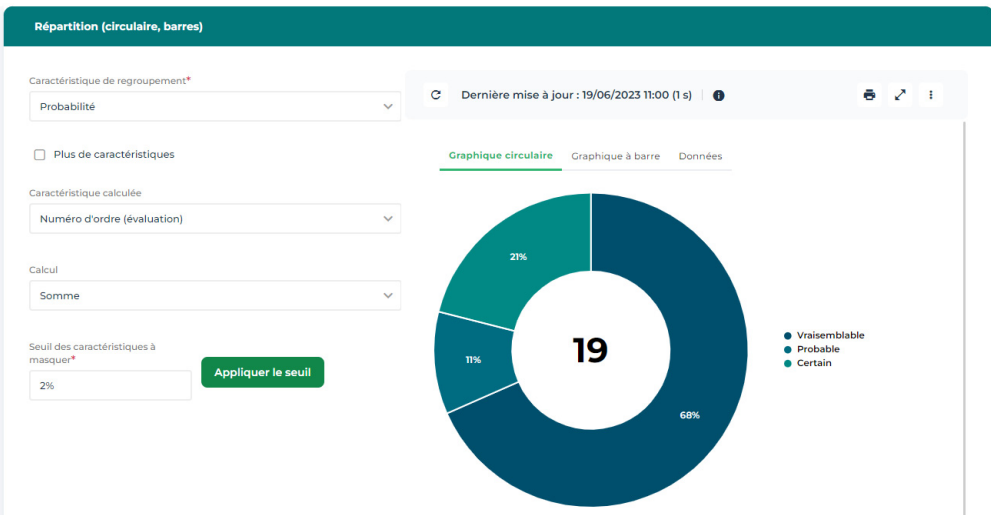
Les rapports instantanés offrent une représentation graphique statistique des données. Vous pouvez générer des rapports instantanés sur une sélection d'évaluations afin de visualiser graphiquement certaines données ou comparer les évaluations sur des caractéristiques spécifiques.

Pour lancer un rapport instantané sur un ensemble d'évaluations d'un risque :

1. Affichez les propriétés du risque évalué et cliquez sur la page **Évaluation**.
2. Sélectionnez les évaluations.
3. Cliquez sur le bouton **Rapport instantané**.
4. Sélectionnez le type de rapport à créer puis, si nécessaire, les caractéristiques à analyser.

Exemple

Ci-dessous un exemple de rapport de type “Répartition" sur les évaluations d’un risque. A partir des caractéristiques sélectionnées (ici, l’impact du risque), le rapport offre une représentation graphique des résultats obtenus.



Pour plus de détails sur les rapports instantanés, voir Gérer les rapports instantanés.

Générer des rapports dédiés

Outre les rapports instantanés, **Hopex Enterprise Risk Management** offre des rapports types dédiés qui facilitent l’analyse des risques évalués. Pour plus de détails, voir Rapports concernant les risques.

MAÎTRISE ET TRAITEMENT DU RISQUE

Hopex Enterprise Risk Management permet de définir des stratégies de maîtrise du risque et de mettre en place des plans d'actions pour traiter le risque.

- ✓ Gérer le risque
- ✓ Traiter le risque

GÉRER LE RISQUE

Pour définir la stratégie de gestion du risque :

1. Voir Accéder à tous les risques.
2. Dans la page de propriétés du risque, sélectionnez la page **Maîtrise**.
3. Définissez ici :
   - votre **Stratégie** de gestion des risques
   - les **Contrôles** permettant de prévenir, détecter et corriger.

Spécifier la stratégie de maîtrise du risque

Pour définir la stratégie de maîtrise du risque :

- Dans la section **Stratégie** de la page **Maîtrise** du risque, définissez la stratégie permettant de faire face au risque :
  - ***Acceptation***
    Il s'agit de la stratégie de gestion du risque qui consiste en la décision éclairée d'accepter le risque. Tant qu'aucune volonté de traitement du risque ne se manifeste, cette stratégie ne permet pas de protéger l'organisation contre le risque.
  - ***Réduction***
    Il est possible de réduire la fréquence du risque, en mettant en place des contrôles supplémentaires ou de réduire l'impact de ses conséquences si le risque survient.
  - ***Transfert*** (sous-traitant)
    Le risque peut être partagé avec des partenaires, en particulier lorsque ceux-ci ont plus de compétences pour maîtriser le risque.
  - ***Assurance***
    En complément de toutes les approches précédentes, il est souvent nécessaire de recourir à une assurance, en particulier, pour les risques dont la fréquence est faible, mais l'impact élevé.

Les différents scénarios possibles sont étudiés en mettant en regard leurs aspects positifs et négatifs, afin de choisir un scénario compatible avec le niveau de maîtrise du risque souhaité.

Spécifier l'appétence au risque

Pour spécifier le niveau de risque accepté par l'organisation :

- Dans la section **Stratégie** de la page **Maîtrise** du risque, renseignez le champ **Appétence au risque**.

  📖 *L'appétence au risque est le niveau de risque qu'une organisation est prête à accepter pour atteindre ses objectifs, avant toute mesure prise pour atténuer le risque.*

Mettre en place des contrôles

📖 *Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.*

Pour définir des contrôles sur le risque :

1. Dans les propriétés du risque, sélectionnez la page **Maîtrise**.
2. Dans la section **Contrôles**, définissez des contrôles, correctifs ou préventifs.

☛ *la nature du contrôle (correctif ou préventif) est à spécifier dans les propriétés du contrôle.*

- *La mise en place de contrôles préventifs pour réduire la fréquence et l'impact du risque peut constituer une solution pour réduire le risque.*
- *La mise en place de contrôles correctifs permet de ramener le niveau de risque à un niveau acceptable.*

TRAITER LE RISQUE

Pour indiquer les plans d'action qui permettent de prévenir ou traiter le risque :

1. Dans la barre de navigation, sélectionnez **Risques**.
2. Dans les propriétés d'un risque, sélectionnez la page **Plans d'action**.

> 🕮 *Un plan d'action est constitué d'une série d'actions, avec pour objectif de réduire les risques et les événements ayant un impact négatif sur l'activité de l'entreprise.*
>
> ☛ *Pour plus de détails sur les plans d'action, voir Utiliser les plans d'action.*

Cette page permet de dresser la liste des plans d'action mis en place : par exemple, pour la création ou l'amélioration d'un contrôle, la gestion d'une crise liée à l'occurrence d'un incident ou la refonte d'un processus dans le but de l'améliorer.

Un workflow est créé automatiquement à la création du plan d'action. Pour plus de détails, voir Workflows liés aux plans d'action.

RAPPORTS CONCERNANT LES RISQUES

Différents types de rapports proposés en standard par **Hopex Enterprise Risk Management** visent à analyser les risques et types de risque.

☛ *Vous pouvez créer des rapports à partir de ces rapports types via le menu **Rapports** de la barre de navigation. Pour plus de détails, voir Créer un rapport.*

- ✓ Rapport d'environnement d'un risque
- ✓ Rapport d'impacts d'un risque
- ✓ Décomposition des impacts d'un type de risque
- ✓ Analyse nœud papillon
- ✓ Analyse du profil de risque par contexte
- ✓ Les rapports d'agrégation
- ✓ Les rapports de suivi des risques
- ✓ Les rapports d'Efficacité de la gestion du risque

RAPPORT D'ENVIRONNEMENT D'UN RISQUE

☛ *Ce rapport est disponible pour tous les profils ERM.*

Vous pouvez choisir d'afficher les éléments suivants pour un risque donné :

- le contexte du risque
  - catégorie de processus
  - processus
  - applications
  - acteurs
  - lignes métier
- les objets stratégiques impactés par le risque (objectifs)
- les conséquences du risque (risques associés)
- les contrôles préventifs visant à remédier au risque

  🕮 *Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.*
- incidents

  🕮 *Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.*
- les plans d'action et actions

Chemin d'accès

Fenêtre de propriétés d'un risque (**Rapports > Environnement d'un risque**).

Paramètres du rapport

Paramètres	Type du paramètre	Contraintes
Risque	1 risque	Obligatoire
Contexte du risque (catégorie de processus, processus, applications, entités, lignes métier)	Case à cocher	Facultatif
Objectifs	Case à cocher	Facultatif
Risques associés	Case à cocher	Facultatif
Contrôles	Case à cocher	Facultatif
Incidents	Case à cocher	Facultatif

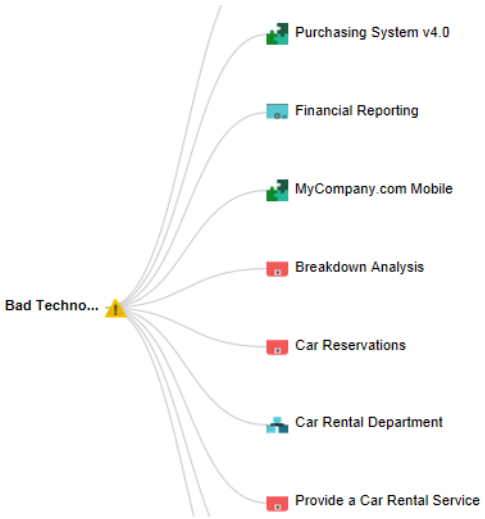
Paramètres	Type du paramètre	Contraintes
Constats	Case à cocher	Facultatif
Plans d'action	Case à cocher	Facultatif
Actions	Case à cocher	Facultatif

Créer un rapport d'environnement de risque

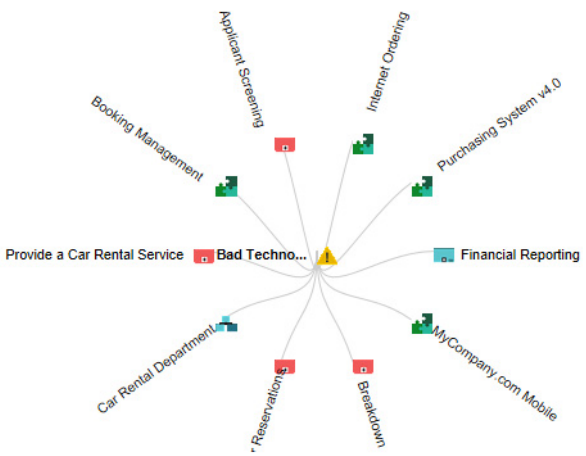
Pour afficher le rapport d'environnement d'un risque :

1. Dans la fenêtre de propriétés d'un risque, sélectionnez la page **Rapports > Environnement d'un risque**.
2. Dans la section **Paramètres**, sélectionnez les types d'objets que vous souhaitez afficher.

3. Dans le champ **Affichage du rapport**, indiquez si vous souhaitez afficher les objets de l'environnement du risque de manière :
   - horizontale



   - circulaire (autour du risque sélectionné)



4. Cliquez sur le bouton **Rafraîchir**.

A partir de ce diagramme, vous pouvez :

- replier/déplier des branches
- ouvrir la page de propriétés de l'objet sélectionné

RAPPORT D'IMPACTS D'UN RISQUE

Ce rapport est un dendrogramme affichant tous les éléments impactés d'un risque.

Chemin d'accès

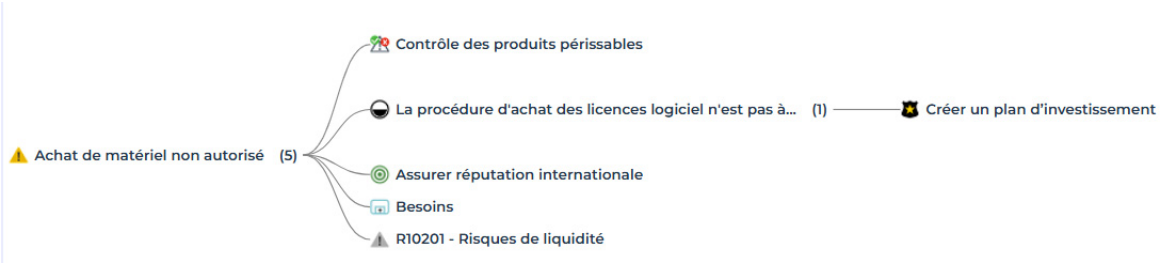
Fenêtre de propriétés d'un risque :

- **Rapports > Impacts d'un risque**, ou
- **Vue d'ensemble**

Paramètres du rapport

Paramètres	Type du paramètre
Risque	1 risque

Exemple



DÉCOMPOSITION DES IMPACTS D'UN TYPE DE RISQUE

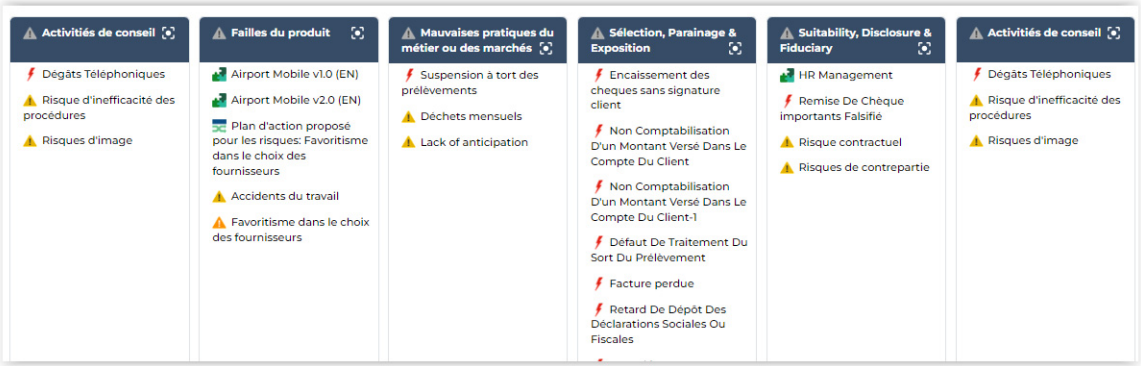
Le rapport "Décomposition des impacts de type de risque" permet de visualiser les impacts du type de risque sélectionné.

Pour accéder à ce rapport :

1. Dans l'arbre de navigation, cliquez sur **Risques > Par type de risque**.
2. Ouvrez les propriétés d'un type de risque et sélectionnez la page **Rapports > Décomposition des impacts d'un type de risque**.

Vous pouvez :

- filtrer les types d'objets à afficher (risque, application, contrôle, incident, plan d'action)
- sélectionner une période de temps



☛ *Pour plus de détails sur les rapports de décomposition, voir Manipuler un rapport de décomposition.*

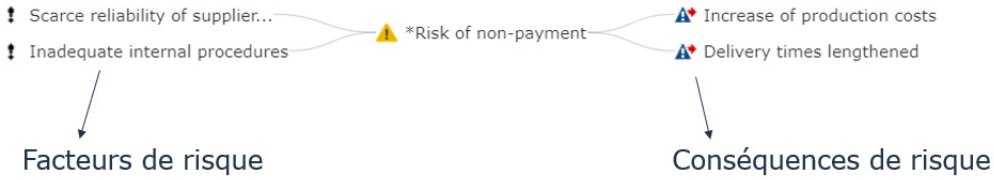
ANALYSE NŒUD PAPILLON

L'analyse nœud papillon permet d'illustrer les causes et conséquences d'un risque.

Chemin d'accès

Fenêtre de propriétés d'un risque (**Rapports > Analyse nœud papillon**)

Exemple



Analyse du profil de risque par contexte

Ce rapport présenté sous forme de tableau de bord permet d'identifier les risques. Il affiche la répartition des risques sur plusieurs axes : par processus, par type de risque, par entité et par objectif.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les risques qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les objectifs.

Paramètres	Type du paramètre	Critère de sélection des risques
Date de début	Date	Non obligatoire.
Date de fin	Date	Date courante par défaut
Type de risque du périmètre	type de risque	Non obligatoire.
Entités du périmètre	entité	Non obligatoire.
Processus du périmètre	processus	Non obligatoire.
Objectifs du périmètre	objectifs	Non obligatoire.

Contenu du rapport

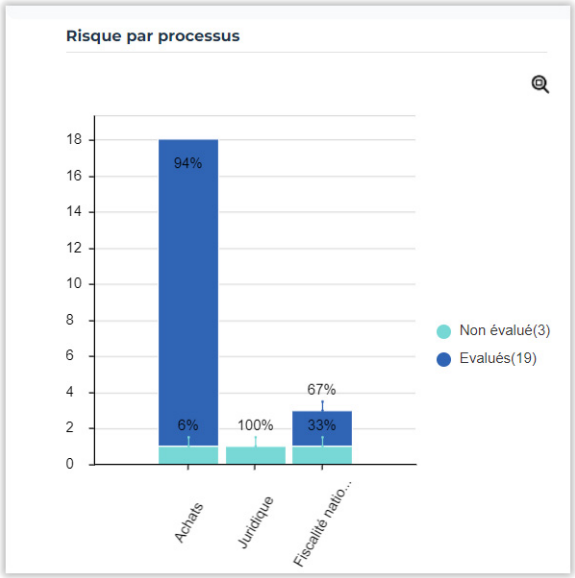
La partie supérieure présente la répartition des risques :

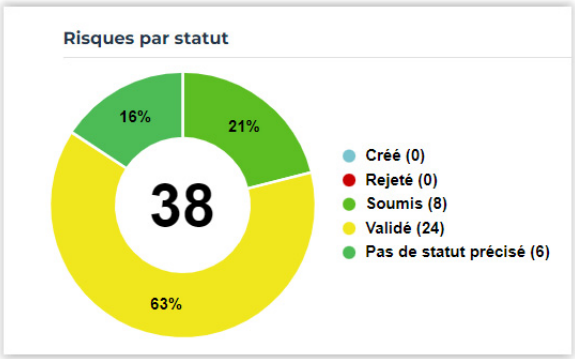
- par processus (évalués/non évalués)
- par type de risque (évalués/non évalués)
- par entité (évalués/non évalués)
- par objectif (évalués/non évalués)
- par statut (créés, soumis, validés, rejetés)

La partie inférieure présente la répartition des risques sur les critères suivants :

- Traitement du risque (risques avec contrôles/sans contrôle)
- Évaluation du risque (évalués/non évalués)
- Déclaration mensuelle des risques (évalués/non évalués)

Exemples





Pour obtenir la liste des risques qui composent un secteur ou une barre d'histogramme :

- Cliquez que le secteur (ou la barre d'histogramme) qui vous intéresse.
  La liste des risques pris en compte est présentée en bas de la zone d'édition.

  ☛ *Pour plus de détails sur le fonctionnement des rapports instantanés, voir **Hopex Common Features**.*

LES RAPPORTS D'AGRÉGATION

Risque résiduel par type de risque

Ce rapport présente sous forme de diagramme à barres empilées :

- sur l'axe horizontal : le nombre de risques par type de risque

  📖 *Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.*

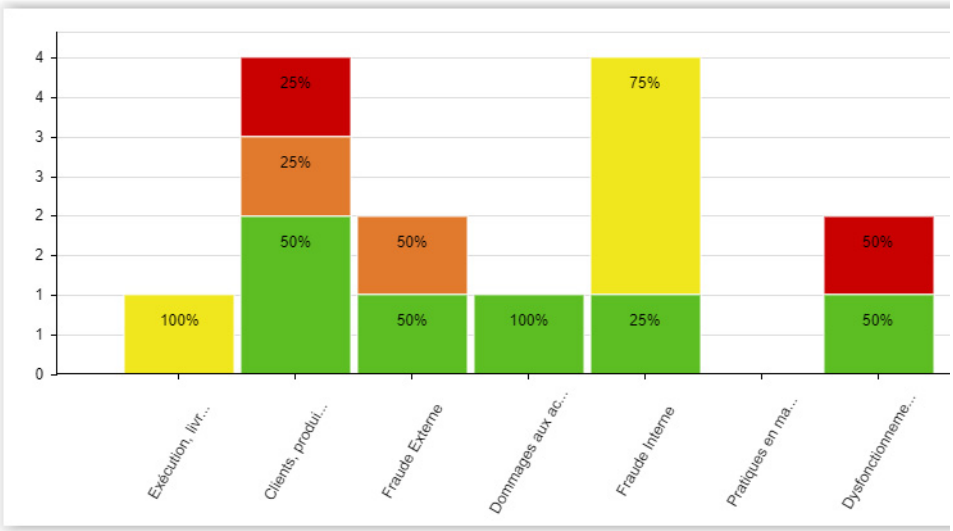
- sur l'axe vertical : le nombre de risques par niveau de risque résiduel

  📖 *Le risque résiduel (ou risque net) est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management.*

Chemin d'accès

Barre de navigation > Rapports

Exemple



Cartographie de risque inhérent et résiduel

Ce rapport permet au Risk Manager ainsi qu'à tous les contributeurs de visualiser l'impact et la probabilité d'un ensemble de risques. Son objectif est de connaître les risques qui nécessitent d'être surveillés.

☛ *L'agrégation consiste à calculer une valeur agrégée des valeurs renseignées sur chaque risque à partir des évaluations.*

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Pour spécifier les paramètres du rapport :

- Après avoir créé le rapport, dans l'onglet **Paramètres**, spécifiez la **Liste des risques** devant alimenter le rapport.

Contenu de la cartographie

Cette cartographie présente les valeurs agrégées des risques sans duplication des risques (les contextes n'étant pas pris en compte).

Cartographie risque inhérent et résiduel par contexte

Ce rapport permet de visualiser la répartition des risques en fonction de différents critères :

- Risque inhérent
  - **Impact** : caractérise l'impact du risque lorsqu'il se manifeste
  - **Probabilité** : caractérise la probabilité que le risque se manifeste
- Risque résiduel
  - **Risque inhérent** : est le produit de la valeur de l'impact par la valeur de la probabilité. Cette caractéristique donne un appréciation des conséquences du risque.
  - **Dispositif de maîtrise du risque** : donne une appréciation globale du niveau de maîtrise du risque.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de définir les données en entrée du rapport.

Paramètres	Type du paramètre	Critère de sélection des risques
Date de début	Date	Non obligatoire.
Date de fin	Date	Date courante par défaut.
Liste de types de risques	type de risque	Non obligatoire.
Liste d'acteurs	entité	Non obligatoire.
Liste de processus	processus	Non obligatoire.
Liste d'objectifs	objectifs	Non obligatoire.
Liste de dispositifs de contrôle	dispositifs de contrôle	Non obligatoire.

☛ *Si vous renseignez un type de risque et une entité, vous obtenez les risques relié à ce type de risque OU à cette entité (L'opérateur OR est utilisé, et non pas AND).*

☛ *Pour activer les dispositifs de contrôle : à partir du menu principal, sélectionnez **Paramètres > Options** puis **Compatibilité > Solutions HOPEX > Activation des dispositifs de contrôle**.*

Exemple de rapport

Risque inhérent

Probabilité \ Impact	Très bas	Bas	Moyen	Elevé	Très élevé
Certain	0	0	0	0	0
Probable	0	1	3	2	1
Vraisemblable	0	1	1	1	0
Possible	0	3	1	0	0
Rare	0	0	2	0	0

Risque résiduel

Risque inhérent \ Dispositif de maitrise du risque	Efficace	Perfectible	Peu efficace	Inefficace	Inexistant
Très élevé	0	1	0	0	0
Elevé	1	1	1	1	2
Moyen	1	1	1	1	0
Bas	2	1	1	0	1
Très bas	0	0	0	0	0

☛ *Seules les dernières valeurs des évaluations de risques sont prises en compte pour chaque contexte Risque x Entité.*

Évaluation des risques par contexte

Ce rapport permet d'afficher le résultat des évaluations de risques par :

- catégorie de processus
- objectif
- acteur
- type de risque

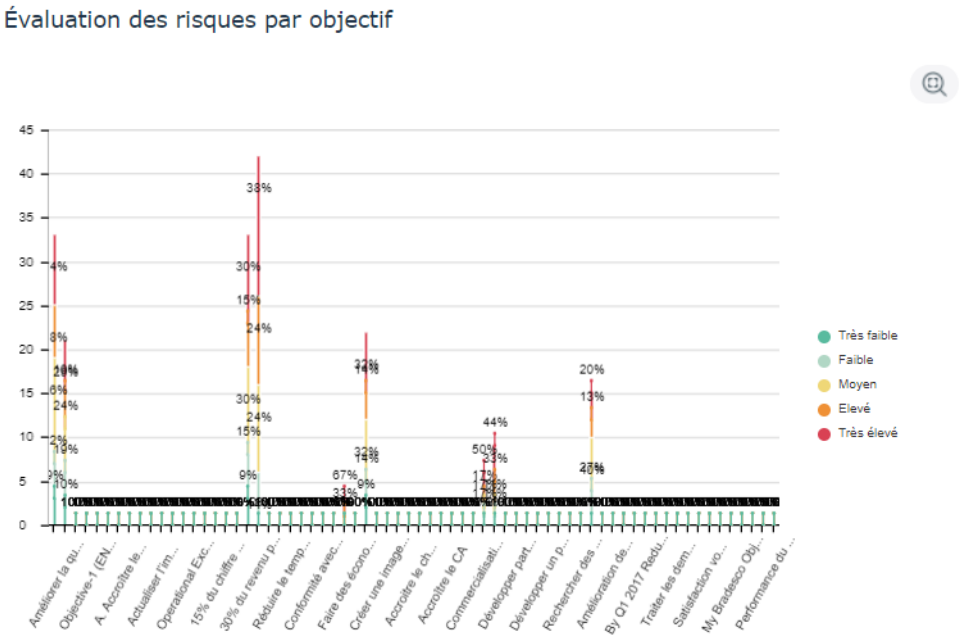
Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Paramètres	Type du paramètre
Date de début	Date
Date de fin	Date
Type du contexte	Catégorie de processus Objectif Acteur Type de risque

Exemple



Niveau de risque global par processus

Ce rapport affiche un tableau des risques liés aux objectifs des catégories de processus données en paramètre.

Il affiche les valeurs du risque résiduel pour chaque risque de chaque catégorie de processus.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Paramètres	Type du paramètre	Critère de sélection des risques
Date de début	Date	Non obligatoire
Date de fin	Date	Date courante par défaut
Liste de catégories de processus	Catégorie de processus	Non obligatoire

Exemple de rapport

Catégories de processus	Objectifs	Risque	Appétence au risque moyenne	Niveau de risque résiduel moyen courant	Niveau de risque min.	Niveau de risque max.	Plan d'action
*Processus de l'Aéroport	Double des ventes en 3 ans	Conscience insuffisante du marché	Très faible	Moyen	Moyen	Moyen	Review marketing plan (EN)
		Crise économique	Moyen	Moyen	Moyen	Moyen	
		Retards de production	Très faible	Très élevé	Très élevé	Très élevé	Proposed Action plan for Risk: Retards de production

Niveau de risque global par entité

Ce rapport présente les risques liés aux objectifs des entités spécifiées en paramètre.

Il affiche les valeurs du risque résiduel de chaque risque dans chaque entité.

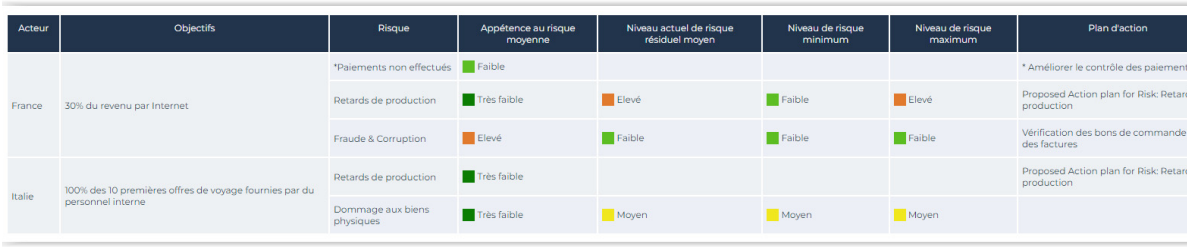
Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Paramètres	Type du paramètre	Critère de sélection des risques
Date de début	Date	Non obligatoire.
Date de fin	Date	Date courante par défaut.
Liste d'entités	Entités	Non obligatoire.

Exemple de rapport



Acteur	Objectifs	Risque	Appétence au risque moyenne	Niveau actuel de risque résiduel moyen	Niveau de risque minimum	Niveau de risque maximum	Plan d'action
France	30% du revenu par Internet	*Paiements non effectués	Faible				* Améliorer le contrôle des paiement
		Retards de production	Très faible	Elevé	Faible	Elevé	Proposed Action plan for Risk: Retar production
		Fraude & Corruption	Elevé	Faible	Faible	Faible	Vérification des bons de commande des factures
Italie	100% des 10 premières offres de voyage fournies par du personnel interne	Retards de production	Très faible				Proposed Action plan for Risk: Retar production
		Dommage aux biens physiques	Très faible	Moyen	Moyen	Moyen	

Rapport d'agrégation

Ce rapport permet de consulter la synthèse des niveaux de risques pour une arborescence d'objets (ex : hiérarchie des entités, hiérarchie des types de risques) ainsi que le détail des niveaux de risques de chaque risque rattaché aux feuilles de l'arborescence.

Le bouton **Lancer l'agrégation** permet de générer les données d'agrégation.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de définir les données en entrée du rapport.

Paramètres	Type du paramètre	Contraintes
Date de début	Date	Critère de sélection des risques. Non obligatoire.
Date de fin	Date	Critère de sélection des risques, fixée à la date courante.
Racine du contexte	L'objet racine peut être de type Entité, Processus ou Type de risque.	Racine des objets présentés en ligne dans le rapport. ***Obligatoire***.
Schéma d'agrégation	Schéma d'agrégation à appliquer	***Obligatoire.***
Caractéristiques évaluées	Caractéristiques d'évaluation.	Liste des métriques présentées en colonne dans le rapport. Proposées par défaut en fonction du schéma d'agrégation sélectionné. ***Obligatoire***.

Exemple de rapport

L'exemple ci-dessous permet de visualiser les valeurs agrégées des risques sur des entités.

En dépliant une entité, il est possible de visualiser l'agrégation des valeurs sur chacun des risques reliés à l'entité.

	Risque brut moy	Dispositif de maîtrise du risque moy	Risque résiduel moy
*Mega Group	Moyen	Peu efficace	Elevé
Filiales Régionales	Moyen	Peu efficace	Elevé
France	Elevé	Inefficace	Elevé
Favoritisme dans le choix des fournisseurs	Elevé	Inexistant	Elevé
Emissions de CO2	Moyen	Peu efficace	Moyen
*Paiements non effectués	Moyen	Peu efficace	Moyen
Application piratée	Très bas	Peu efficace	Faible
Fraude & Corruption	Très élevé	Inexistant	Très élevé
Catastrophe naturelle	Elevé	Inexistant	Elevé
Etats-Unis	Moyen	Peu efficace	Moyen
Belgique	Moyen	Peu efficace	Moyen
Japon	Elevé	Inefficace	Elevé

LES RAPPORTS DE SUIVI DES RISQUES

Statistiques sur une session d'évaluation

Ce rapport affiche les données des questionnaires d'une session d'évaluation donnée et permet d'analyser la répartition des réponses.

Chemin d'accès

Propriétés d'une session d'évaluation > Page Rapports > Statistiques

Paramètres

Paramètres	Remarques
Campagne	Obligatoire
Session	Obligatoire

Exemple de rapport

	Nombre de réponses	% Réponses
Dispositif de maîtrise du risque	3	100%
Très fort	0	0%
Fort	0	0%
Moyen	0	0%
Faible	1	33%
Très faible	2	66%
Probabilité	3	100%
Rare	0	0%
Possible	1	33%
Vraisemblable	2	66%
Probable	0	0%
Certain	0	0%
Impact	3	100%

Résultat

Une arborescence affiche :

- en ligne : les questions /réponses, ainsi que les répondants

  ☛ *En dépliant une réponse, vous obtenez les risques sur lesquels porte la réponse ainsi que le nom des répondants.*

- en colonne : pour chaque question/réponse, le nombre de répondants

Cette arborescence permet de visualiser qui a répondu quoi pour quelle question.

LES RAPPORTS D'EFFICACITÉ DE LA GESTION DU RISQUE

Analyse des risques et des incidents

Ce rapport permet au Risk Manager de visualiser :

- les risques affectant l'entité dont il est responsable ainsi que ses sous-entités
- les objets de l'environnement de chaque risque (processus métier, ligne métier par exemple)
- l'état de la mitigation des risques gérés
  - les contrôles de mitigation
  - les incidents qui matérialisent ces risques
  - les plans d'action concernant les risques

Si, par exemple, le risque se matérialise par des incidents, le Risk Manager peut visualiser quels contrôles vérifier et quels plans d'action modifier.

Chemins d'accès

Barre de navigation > Rapports

Paramètres

Paramètres	Contraintes
Éléments à risque	Obligatoire

Contenu du rapport

Le rapport présente, en colonnes :

- les éléments à risque (par exemple sites ou processus)
- les risques associés
- la date de la dernière évaluation du risque
- les plans d'action à mettre en oeuvre
- la date de fin du plan d'action
- les éventuels incidents
- la date de survenance de l'incident

Exemple

Elément à risque	Risque	Dernière évaluation	Plan d'action	Date de fin réelle	Incident	Date d'événement
Belgique	Budget insuffisant	04/05/2023				
	Cryptage des données	22/02/2022	Proposed Action plan for Risk: Data encryption (EN)			
	Dépenses non autorisées	04/05/2023	Examen annuel des comptes	31/03/2023	Indisponibilité totale d'un Gab	22/11/2022
	Fraude & Corruption	04/05/2023	Vérification des bons de commande et des factures			
	Procédures du département d'achat très vague	04/05/2023			Remise De Chèque importants Falsifié	29/11/2022
					Sinistre Auto	09/09/2022
France	Application piratée	04/05/2023			* Perte de données	19/03/2021
					Perte irreversible de permis de conduire	01/05/2021
					Produits non livrés au clients	25/10/2022
	Catastrophe naturelle	04/05/2023	Souscription de polices d'assurance	31/07/2021		
	Emissions de CO2	04/05/2023	Mise en place de capteurs de CO2	21/05/2021		
	Favoritisme dans le choix des fournisseurs	04/05/2023	Plan d'action proposé pour les risques: Favoritisme dans le choix des fournisseurs			
	Fraude & Corruption	04/05/2023	Vérification des bons de commande et des factures			
	Retards de production	04/05/2023	Proposed Action plan for Risk: Retards de production			

Matrice de couverture des contrôles et des risques

En tant que Risk Manager vous avez besoin de vérifier si les risques de votre périmètre ont des contrôles de mitigation associés. Ceci doit vous permettre de prioriser vos efforts de conception de contrôles.

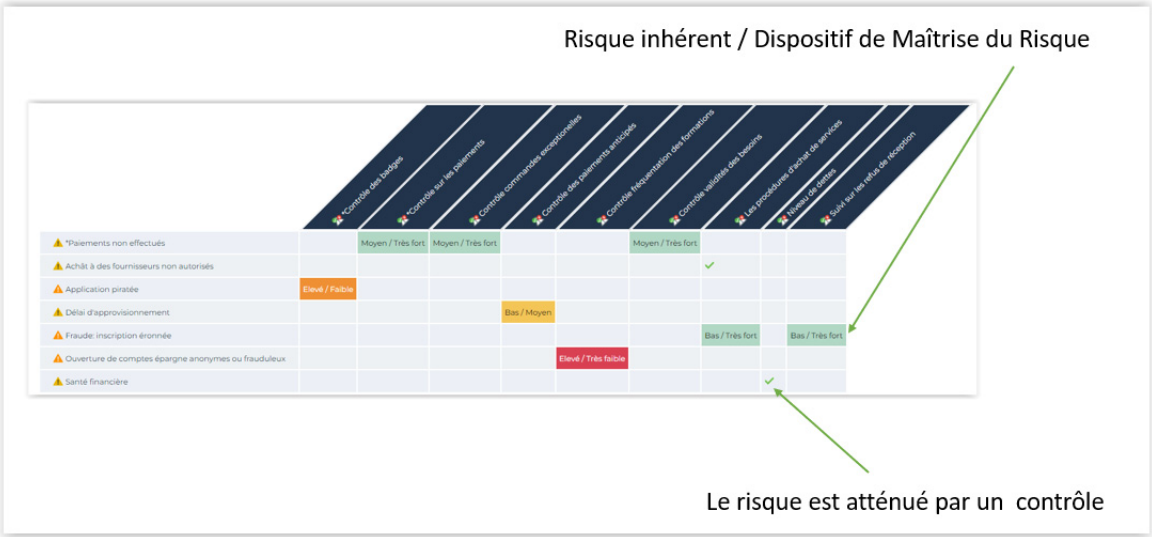
Chemin d'accès

Barre de navigation > Rapports

Contenu de la matrice

Cette matrice permet d'afficher:

- en ligne : les risques entrant dans le périmètre du Risk Manager
- en colonne : les contrôles ayant pour but d'atténuer ces risques



Lorsque le risque est atténué par un contrôle et qu'une évaluation a déjà été réalisée, les valeurs "Risque inhérent / Dispositif de maîtrise du risque" sont affichées à l'intersection du risque et du contrôle. Ces valeurs correspondent aux valeurs obtenues lors de la dernière évaluation du risque.

> 🕮 *Le risque inhérent (ou risque brut) est le risque auquel une entité est exposée en l'absence de mesures correctives par le management pour en modifier la probabilité d'occurrence ou l'impact, par opposition au risque résiduel.*
>
> 🕮 *Le niveau de Dispositif de Maîtrise du Risque permet de caractériser l'efficacité des contrôles visant à atténuer le risque.*

Tendance des risques

Ce rapport présente :

- la moyenne du risque résiduel des trois dernières années
- la projection du risque résiduel de l'année à venir.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de définir le contexte des risques présentés.

Paramètres	Type du paramètre	Contraintes
Contexte du rapport	Type de risque, entité, processus, objectifs	Critère de sélection des risques présentés en ligne. Non obligatoire.

Exemple de rapport

	2021	2022	2023	Evolution moyenne	Plans d'action	Planifié 2024	Evolution prévue
Favoritisme dans le choix des fournisseurs		Très élevé	Faible	↘	Oui	Très faible	↘
Emissions de CO2	Elevé	Elevé	Moyen	↘	Oui	Très faible	↘
Application piratée		Elevé	Faible	↘	Non	Très faible	↘
Catastrophe naturelle		Moyen	Faible	↘	Oui	Très faible	↘
Fraude & Corruption	Très faible	Elevé	Très faible	→	Oui	Très faible	↘
Retards de production		Elevé	Très élevé	↗	Oui	Très élevé	↗

Calcul du résultat

Méthode de calcul

Evolution des risques =

Risque résiduel Année N + ((Risque résiduel Année N – Risque résiduel Année N-2)/ 2)

Valeurs internes

Nom de la valeur	Valeur interne
Très bas	1
Bas	16

Moyen	81
Elevé	256
Très élevé	625

Exemple

Evolution des risques = Elevé + ((Elevé – Très Elevé)/2)

Evolution des risques = 256 + ((256 – 625)/2)

Evolution des risques = 71,5 (arrondi au seuil le plus proche = 81)

Evolution des risques = Moyen

HOPEX LDC

Guide d’utilisation

HOPEX Aquila 6.2

Bizzdesign

SOMMAIRE

Sommaire

COLLECTE DES INCIDENTS

L'incident constitue l'élément de base de la collecte des données concernant le risque opérationnel.

> 🕮 *Un incident est un fait de source interne ou externe ayant une incidence sur l'organisation. Il constitue l'élément de base de la collecte des données concernant le risque opérationnel.*

Hopex LDC (Loss Data Collection) vous permet d'organiser le suivi des incidents et des pertes, d'identifier leurs causes et de mesurer leur impact.

Le système gère le cycle de vie complet des incidents : vous disposez d'une traçabilité complète, avec l'historique précis des enregistrements.

Le Manager GRC / le gestionnaire des incidents et des pertes peut analyser l'incident avant de valider les données. Il peut visualiser les résultats sous forme de rapports dynamiques. Il peut également décider de grouper les incidents pour éventuellement créer un macro-incident.

- ✓ Profils de connexion à Hopex LDC
- ✓ Gérer les incidents
- ✓ Renseigner les caractéristiques d'un incident
- ✓ Analyser un incident
- ✓ Gérer les macro-incidents
- ✓ Le processus de gestion d'un incident

> ☛ *Pour des informations sur le traitement des incidents, voir la documentation générale sur les plans d'action.*

PROFILS DE CONNEXION À HOPEX LDC

Pour se connecter à **Hopex**, voir Se connecter à Hopex.

Profils	Bureau	Tâches
Gestionnaire des incidents et des pertes (ou Manager GRC)	Hopex GRC	Prépare l'environnement de travail et crée les éléments nécessaires à la gestion des incidents et des pertes. Gère la description de l'environnement : entités et processus, environnement réglementaire, ressources IT. Peut intervenir sur : - les incidents déclarés - les plans d'action et les actions
Contributeur GRC	Contributeurs GRC	Utilise le bureau simplifié HOPEX Explorer. - Déclare des incidents Voir Le bureau des contributeurs GRC.

☛ *Pour plus de détails, voir également Accéder au bureau GRC.*

GÉRER LES INCIDENTS

Accéder aux incidents

Pour accéder aux incidents :

- Dans la barre de navigation, cliquez sur **Incidents**.

Filtrer les incidents

Dans l'onglet **Incidents**, une liste déroulante vous permet de visualiser :

- les **Incidents non clos**

  ☛ *Les incidents non clos correspondent aux incidents qui ont été validés par le Risk Manager.*

- les **Incidents à examiner**

  ☛ *Les incidents à examiner n'ont pas encore été validés par le Risk Manager.*

- les **Incidents orphelins**

  ☛ *Les incidents orphelins sans les incidents qui n'ont pas d'impact connu sur l'organisation (ils n'ont pas d'objet contexte).*

  ☛ *Pour définir les éléments (contextes) impactés par incident donné, ouvrez la page de propriétés de l'incident et sélectionnez **Caractéristiques >Périmètre > Incidents**.*

Accéder aux macro-incidents

Pour accéder aux macro incidents :

- Cliquez sur **Incidents** et sélectionnez l'onglet **Macro-incidents**.

  🕮 *Un macro-incident est un incident qui a des incidences sur plus d'un métier ou d'une société d'un même groupe.*

  ☛ *Pour plus de détails, voir Gérer les macro-incidents.*

Créer un incident

Pour créer un incident :

1. Voir Accéder aux incidents.
2. Cliquez sur **Nouveau**.

   ☛ *Avec le profil "Contributeur GRC", dans la page d'accueil, cliquez sur la tuile **Créer un incident**.*

3. Dans la page de propriétés de l'incident, renseignez :
   - son **Nom**.
   - l'**Entité du déclarant**.

     🕮 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un*

niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.

- la **Date de découverte**
- la **Date d'événement**
- une **Description**

☛ *Pour plus de détails sur ces caractéristiques, voir Renseigner les caractéristiques d'un incident.*

4. Cliquez sur **OK**.

RENSEIGNER LES CARACTÉRISTIQUES D'UN INCIDENT

Pour modifier les caractéristiques d'un incident :

1. Voir Accéder aux incidents.
   La liste des incidents que vous avez déclarés apparaît dans la zone d'édition.
2. Dans la page **Caractéristiques** des propriétés de l'incident que vous souhaitez modifier, renseignez les champs suivants :
   - **Macro-incident** : pour relier l'incident courant à un Macro-Incident existant ou nouveau.

     📖 *Un macro-incident est un incident qui a des incidences sur plus d'un métier ou d'une société d'un même groupe.*

     ☛ *Pour plus de détails, voir Gérer les macro-incidents.*
   - **Statut** : indique le statut courant de l'incident dans le processus de gestion des incidents.

     ☛ *Le **Statut** apparaît en grisé parce qu'il est géré par le workflow associé à l'incident. Pour plus de détails, voir Le processus de gestion d'un incident.*
   - **Date de déclaration**, **Date de découverte** et **Date d'événement** : constituent les dates clés de l'incident.

     ☛ *Pour spécifier une date, servez-vous du calendrier à droite du champ.*

     ☛ *Les dates de déclaration et de découverte de l'incident peuvent être distinctes, la date de déclaration pouvant être postérieure à la date de découverte.*
   - **Nature** : vous pouvez saisir ici la nature (financière ou non) de l'incident.
   - **Quasi-incident** : case à cocher lorsqu'il s'agit d'un *quasi-incident*.

     📖 *Un quasi-incident est un incident qui ne s'est traduit ni en dommages corporels ni en dommages matériels mais qui en avait le potentiel.*
   - **Description** : est un commentaire qui décrit l'incident.

Voir aussi : Enregistrer les montants liés à l'incident

ENREGISTRER LES MONTANTS LIÉS À L'INCIDENT

Une fois que l'incident est déclaré, il est possible d'enregistrer les montants liés à l'incident et ses conséquences, par exemple les *pertes*.

> 🕮 *Une perte est la conséquence financière négative d'un événement.*
>
> 🕮 *Un gain est la conséquence financière positive d'un incident.*
>
> 🕮 *Une provision est un montant qui diminue le résultat pour faire face à un risque ou une charge incertaine. Plusieurs provisions peuvent concerner un seul et même risque.*
>
> 🕮 *Une récupération est une somme qui dans certaines circonstances vient réduire le montant des pertes liées au risque opérationnel. Elle permet de récupérer une partie des sommes engagées dans l'événement.*

Voir aussi : Renseigner les caractéristiques d'un incident.

Accéder à l'analyse financière d'un incident

Pour accéder aux données d'analyse financière d'un incident :

1. Voir Accéder aux incidents.
   La liste des incidents que vous avez déclarés apparaît dans la zone d'édition.
2. Sélectionnez l'incident que vous souhaitez modifier.
3. Dans la page de propriétés de l'incident, sélectionnez la page **Analyse financière**.
   Les montants totaux apparaissent dans la section **Montants totaux**.

   > ☛ *Pour plus de détails sur les montants totaux d'un incident, voir Visualiser les montants calculés liés à l'incident.*

Saisir une perte

Pour saisir une *perte* :

> 🕮 *Une perte est la conséquence financière négative d'un événement.*

1. Voir Accéder aux incidents.
2. Dans les propriétés de l'incident, sélectionnez la page **Analyse financière**.

   > ☛ *Pour plus de détails, voir Accéder à l'analyse financière d'un incident.*
3. Dépliez la section **Pertes, Gains, Récupérations et Provisions**.
4. Sélectionnez l'onglet **Pertes** et cliquez sur le bouton **Nouveau**.
   Une nouvelle perte apparaît dans la liste.
5. Sélectionnez la nouvelle perte et cliquez sur **Propriétés**.

6. Dans l'onglet **Caractéristiques**, renseignez les champs suivants :
   - **Nom**
   - **Description** : commentaire concernant la perte.
   - **Date d'effet**
   - **Nature** : "Atteinte au biens", "Dépréciation (monétaire)", "Pertes non recouvertes", "Responsabilité légale", etc.
   - **Compte** dans lequel la perte est comptabilisée.

     ☛ *Pour plus de détails sur la notion de compte, voir L'environnement des contrôles.*
7. Cliquez sur le bouton à côté du champ **Montant (local)** pour sélectionner la devise de la perte.

   ☛ *Les montants saisis dans une devise sont convertis dans la devise locale et dans la devise centrale.*

   ☛ *Si aucun taux de change n'a été défini préalablement par l'administrateur, le montant est automatiquement pris en compte dans la devise centrale.*

   ☛ *Si vous n'êtes pas certain du montant, vous pouvez cocher la case **Montant estimé**. Le montant saisi ne sera pas pris en compte dans les **Pertes réelles brutes** de l'incident.*

   ☛ *Les pertes qui portent sur un quasi-incident sont généralement estimées. Il est cependant possible de saisir des pertes réelles.*
8. Dépliez la section **Périmètre**, renseignez éventuellement les informations spécifiques à la perte, par exemple :
   - **Entité** pour lequel cette perte doit être comptabilisée.

   Par défaut, il s'agit de la même entité que celle déclarée pour l'incident.
   - **Ligne métier** concernée par cette perte.

     ☛ *Pour plus de détails sur les éléments qui définissent le périmètre d'un incident ou d'une perte, voir Définir le périmètre d'une perte.*
9. Cliquez sur **Ok**.

Définir le périmètre d'une perte

Le périmètre d'une perte permet de définir la localisation de la perte, donc de l'incident associé et donc d'un risque au sein de l'organisation.

☛ *La description de l'organisation est détaillée dans le chapitre Environnement GRC.*

Le périmètre d'une perte est précisé sur plusieurs types de composants :

- les *entités* concernées par la perte.

  🕮 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.*
- les *lignes métier* concernées par la perte

  🕮 *Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par*

exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.

- les *types de risque* à associer à la perte

  📖 *Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.*

- les *processus métier* et des *processus organisationnels* concernées par la perte.

  📖 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

  📖 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

- les *produits* impactés par la perte.

  📖 *Un produit représente un ou plusieurs articles, objets, biens ou services, résultat d'une activité agricole, industrielle ou de service, qui sont proposés par une entreprise.*

- les *applications* impactées par la perte.

  📖 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

Saisir un gain

📖 *Un gain est la conséquence financière positive d'un incident.*

Pour saisir un gain :

1. Voir Accéder aux incidents.
2. Dans les propriétés de l'incident, sélectionnez la page **Analyse financière**.
3. Dépliez la section **Pertes, Gains, Récupérations et Provisions**.
4. Sélectionnez l'onglet **Gains** et cliquez sur le bouton **Nouveau**.
   Un nouveau gain apparaît dans la liste.
5. Sélectionnez le nouveau gain et cliquez sur **Propriétés**.
   La fenêtre de propriétés du nouveau gain s'ouvre.
6. Dans l'onglet **Caractéristiques**, renseignez les champs suivants :
   - **Nom**
   - **Description** : commentaire concernant le gain.
   - **Date d'effet**
   - **Compte** dans lequel l'incident est comptabilisé.

     ☛ *Pour plus de détails sur la notion de compte, voir L'environnement de conformité.*

7. Dépliez la section **Montant**, renseignez éventuellement les informations concernant le montant du gain.

   ☛ *Les montants saisis dans une devise sont convertis dans la devise locale et dans la devise centrale.*

   ☛ *Si aucun taux de change n'a été défini préalablement par l'administrateur, le montant est automatiquement pris en compte dans la devise centrale.*

   ☛ *Si vous n'êtes pas certain du montant, vous pouvez cocher la case **Montant estimé**. Le montant saisi ne sera pas pris en compte dans les totaux liés à l'incident.*

   ☛ *Les gains portant sur un quasi-incident sont généralement estimées. Il est cependant possible de saisir des gains réels.*

8. Dépliez la section **Périmètre**, renseignez éventuellement les informations spécifiques au gain.

   ☛ *Pour plus de détails sur les éléments qui définissent le périmètre d'un incident, voir Définir le périmètre d'une perte.*

9. Cliquez sur **Ok**.

Enregistrer une récupération

📖 *Une récupération est une somme qui dans certaines circonstances vient réduire le montant des pertes liées au risque opérationnel. Elle permet de récupérer une partie des sommes engagées dans l'événement.*

Il convient de distinguer les *récupérations* provenant des assurances et celles provenant d'autres moyens tels que le recours à la justice, une tierce partie, etc.

Pour saisir une récupération :

1. Voir Accéder aux incidents.
2. Dans les propriétés de l'incident, sélectionnez la page **Analyse financière**.
3. Dépliez la section **Pertes, Gains, Récupérations et Provisions**.
4. Sélectionnez l'onglet **Récupérations** et cliquez sur le bouton **Nouveau**. Une nouvelle récupération apparaît dans la liste.
5. Pour renseigner les information spécifiques à une récupération, procédez de la même manière que pour un gain.

   ☛ *Pour plus de détails, voir Saisir un gain.*

Enregistrer une provision

📖 *Une provision est un montant qui diminue le résultat pour faire face à un risque ou une charge incertaine. Plusieurs provisions peuvent concerner un seul et même risque.*

Pour saisir une *provision* :

1. Voir Accéder aux incidents.
2. Dans les propriétés de l'incident, sélectionnez la page **Analyse financière**.
3. Dépliez la section **Pertes, Gains, Récupérations et Provisions**.

4. Sélectionnez l'onglet **Provision** et cliquez sur le bouton **Nouveau**. Une nouvelle provision apparaît dans la liste.
5. Pour renseigner les information spécifiques à une provision, procédez de la même manière que pour un gain.

☛ *Pour plus de détails, voir Saisir un gain.*

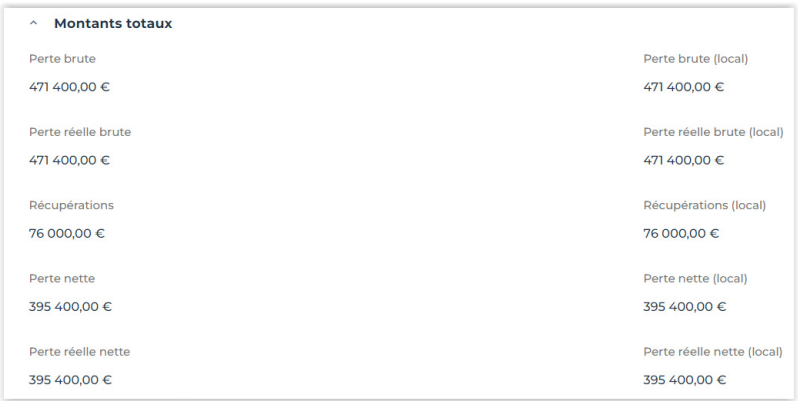
Visualiser les montants calculés liés à l'incident

Pour visualiser les montants calculés liés à un incident :

1. Voir Accéder aux incidents.
2. Dans les propriétés d'un incident, sélectionnez la page **Analyse financière**.

La section **Montants totaux** calcule automatiquement la somme de tous les éléments financiers liés à l'incident (pertes, gains, récupérations et provisions).

☛ *Les montants apparaissent dans la devise centrale et dans la devise locale.*



Les champs suivants donnent des indications chiffrées sur les incidents :

Perte brute

Somme des pertes (estimations comprises) - Gains.

Perte réelle brute

Somme des pertes (estimations non comprises) - Gains.

Récupérations

Somme des récupérations (assurance et non-assurance).

Perte nette

Perte nette = Perte brute - Récupérations

Perte réelle nette

Perte réelle nette = Perte réelle brute - Récupérations.

ANALYSER UN INCIDENT

Une fois les caractéristiques de base d'un incident saisies, vous pouvez compléter des caractéristiques avancées dans le cadre de l'analyse de l'incident.

Ce travail consiste à relier l'incident aux éléments de l'environnement définis par votre organisation.

☛ *Pour plus de détails sur les composants de l'environnement, voir Environnement GRC*

L'analyse qualitative d'un incident

Pour accéder à l'analyse qualitative d'un incident :

1. Voir Accéder aux incidents.
2. Ouvrez la page de propriétés de l'incident.
3. Dans la page **Caractéristiques** dépliez la section **Analyse Qualitative**.

Risques et Contrôles

Pour associer un incident à un risque et à un contrôle :

1. Cliquez sur la flèche à droite du champ **Risque matérialisé** et sélectionnez **Relier Risque.**
2. Sélectionnez le risque qui vous intéresse et cliquez sur **OK**.

   🕮 *Un risque est un danger plus ou moins probable auquel est exposée une organisation.*
3. Cliquez sur la flèche à droite du champ **Contrôle défaillant** et sélectionnez **Relier Contrôle**.
4. Sélectionnez le contrôle qui vous intéresse et cliquez sur **OK**.

   🕮 *Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.*

Priorité de l'incident

Pour qualifier la priorité d'un incident :

1. Dans les propriétés d'un incident, sélectionnez la page **Caractéristiques** et dépliez la section **Analyse qualitative**.
2. Renseignez la **Priorité** qui caractérise l'importance relative de l'incident décrit
   - "Haute"
   - "Moyenne"
   - "Basse"

Impact de l'incident

Pour spécifier l'impact d'un incident :

1. Dans les propriétés d'un incident, sélectionnez la page **Analyse qualitative**.
2. Renseignez l'**Impact** qui caractérise l'impact de l'incident sur les éléments de l'environnement
   - "Très élevé"
   - "Elevé"
   - "Moyen"
   - "Bas"
   - "Très bas"

Les facteurs de risque

Beaucoup de *facteurs de risque* sont définis dans le cadre de réglementations internationales, nationales ou inter-professionnelles, ou au sein de l'entreprise elle-même.

> 🕮 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.*

Il est possible d'associer à chaque incident un ou plusieurs *facteurs de risque*, sources de risques ou dangers qui ont intrinsèquement le potentiel de mettre en danger le fonctionnement de l'organisation. Par exemple, des produits chimiques dangereux, des concurrents, des gouvernements, etc.

Pour définir les facteurs de risque associés à un incident :

1. Dans les propriétés d'un incident, sélectionnez la page **Caractéristiques** et dépliez la section **Analyse qualitative**.
2. Cliquez sur l'onglet **Facteur de risque** puis sur le bouton **Relier**.
3. Sélectionnez le facteur de risques associé à l'incident.
4. Cliquez sur **OK**.

Les conséquences de risque

> 🕮 *Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.*

Pour définir les conséquences de risque associées à un incident :

1. Dans les propriétés d'un incident, sélectionnez la page **Caractéristiques** et dépliez la section **Analyse qualitative**.
2. Cliquez sur l'onglet **Conséquence de risque** puis sur le bouton **Relier**.
3. Sélectionnez les conséquences de risques associées à l'incident.
4. Cliquez sur **OK**.

Le périmètre d'un incident

Pour spécifier le périmètre d'un incident :

1. Voir Accéder aux incidents.
2. Dans les propriétés d'un incident, sélectionnez la page **Caractéristiques** et dépliez la section **Périmètre**.

Le périmètre du risque permet de définir la localisation d'un risque au sein de l'organisation.

> ☛ *La description de l'organisation est détaillée dans le paragraphe L'organisation.*

Le périmètre est précisé sur plusieurs types de composants :

- les *entités* concernées par l'incident.

  > 🕮 *Une entité peut être interne ou externe à l'entreprise : une entité interne représente un élément de l'organisation d'une entreprise tel qu'une direction, un service ou un poste de travail. Il est défini à un niveau plus ou moins fin en fonction de la précision à fournir sur l'organisation (cf type d'acteur). Ex : la direction financière, la direction commerciale, le service marketing, l'agent commercial. Une entité externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.*

- les *lignes métier* concernées par l'incident

  > 🕮 *Une ligne métier est une compétence ou un regroupement de compétences qui est d'intérêt pour l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution ou à des activités métier.*

- les *types de risque* à associer à l'incident

  > 🕮 *Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.*

- les *catégories de processus* et *processus* concernés par l'incident.

  > 🕮 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

  > 🕮 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

- les *produits* impactés par l'incident.

  > 🕮 *Un produit représente un ou plusieurs articles, objets, biens ou services, résultat d'une activité agricole, industrielle ou de service, qui sont proposés par une entreprise.*

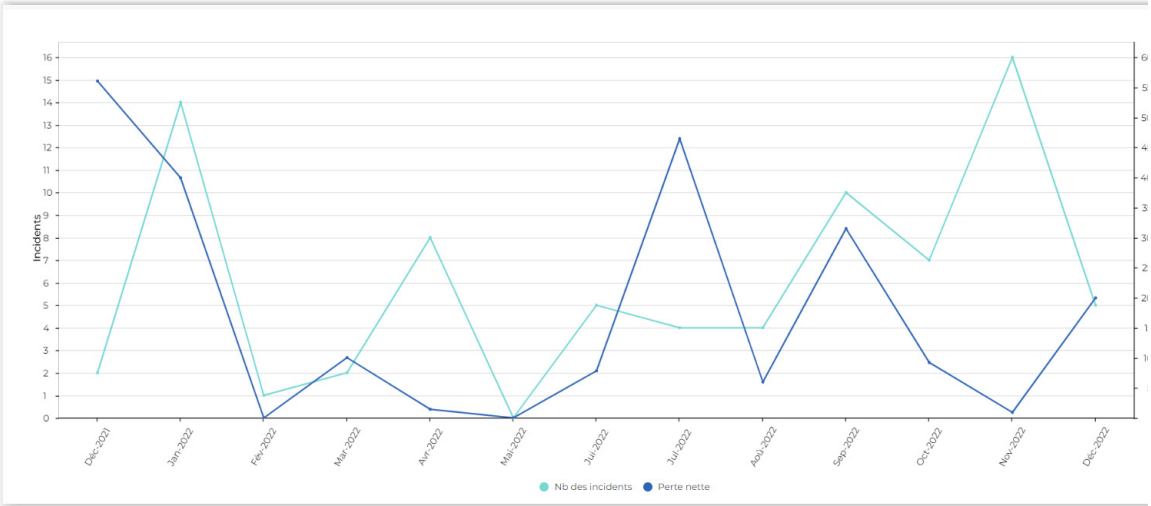
- les *applications* impactées par l'incident.

  > 🕮 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

L'analyse d'impact des incidents

Hopex GRC offre la possibilité d'analyser, sur plusieurs axes, la répartition des incidents liés à un élément de l'environnement.

Pour plus de détails, voir la documentation sur les rapports : Les rapports d'analyse des pertes



GÉRER LES MACRO-INCIDENTS

Un incident ne concerne qu'une seule ligne métier et une seule unité organisationnelle, c'est pourquoi **Hopex GRC** permet de créer des macro-incidents.

Le *macro-incident* permet de représenter un groupe d'incidents qui ont généré des pertes sur différentes lignes métier et/ou sur différentes sociétés du groupe.

> 🕮 *Un macro-incident est un incident qui a des incidences sur plus d'un métier ou d'une société d'un même groupe.*

Par exemple un incident volontaire dans un bâtiment peut avoir des répercussions sur plusieurs lignes métier ou unités organisationnelles du groupe.

Relier un incident à un macro-incident

Vous pouvez relier des incidents à un macro-incident de deux façons :

- depuis la page de propriétés d'un macro-incident, dans l'onglet **Incidents** en reliant des incidents existants.
- depuis un incident (manipulation décrite ci-dessous)

Pour relier un incident à un macro-incident :

1. Voir Accéder aux incidents.
2. Sélectionnez l'incident que vous souhaitez modifier et cliquez sur **Propriétés**.
3. Sélectionnez l'onglet **Caractéristiques**.
4. Cliquez sur la flèche à droite du champ **Macro-Incident** et sélectionnez **Relier Macro-Incident**
5. Sélectionnez le macro-incident qui vous intéresse et cliquez sur **OK**.

> ☛ *Les incidents sont visibles dans la page **Incidents** du macro-incident.*

Créer un macro-incident

> ☛ *Cette fonctionnalité n'est proposés qu'aux Risk Managers et aux gestionnaires des Incidents et des pertes.*

Pour créer un macro-incident :

1. Dans la barre de navigation, cliquez sur **Incidents > Macro-incidents.**
2. Cliquez sur **Nouveau** et saisissez un **Nom**.
3. Cliquez sur **Suivant** et reliez des incidents existants.

> ☛ *Pour plus de détails sur les éléments qui définissent le périmètre, voir Définir le périmètre d'une perte.*

Analyser un macro-incident

Les incidents reliés au Macro-Incident

Pour accéder à la liste des incidents reliés à un macro-incident :

- Dans les propriétés du macro-incident, sélectionnez la page **Incidents**.

> ☛ *Dans la page **Incidents** du Macro-Incident, les champs **Incidents validés**, **Première occurrence** et **Dernière occurrence** sont remplis automatiquement.*

Les montants du Macro-Incident

La section **Montants totaux** de la page de propriétés du macro-incident présente la somme de tous les éléments financiers renseignés pour les incidents reliés au macro-incident.

Les champs suivants sont calculés automatiquement :

- **Perte brute**
  Somme des pertes relatives à l'incident (estimations comprises) - Gains.
- **Perte réelle brute**
  Perte réelle brute = Somme des pertes relatives à l'incident (estimations non comprises) - Gains.
- **Récupérations**
  Somme des récupérations (assurance et non-assurance).
- **Perte nette**
  Perte nette = Perte brute - Récupérations
- **Perte réelle nette**
  Perte réelle nette = Perte réelle brute - Récupérations.

Le rapport d'évolution des pertes

Ce rapport présente l'évolution des pertes nettes par mois des incidents reliés au Macro-incident.

Pour y accéder :

- Dans les propriétés du macro-incident, sélectionnez la page **Evolution des pertes**.

LE PROCESSUS DE GESTION D'UN INCIDENT

Description générale du processus de gestion des incidents

Les étapes du processus de gestion d'un incident sont les suivantes :

- Après avoir renseigné les caractéristiques d'un nouvel incident, le déclarant de l'incident doit **Soumettre** l'incident.
  L'approbateur d'incident reçoit un e-mail et le nouvel incident apparaît avec le statut "Soumis".

  ☛ *Pour définir l'approbateur d'incidents, voir Spécifier les responsabilités au sein d'une entité.*
- Quand un incident a été soumis par son déclarant, l'approbateur d'incident peut **Demander des modifications** de l'incident qui reprend le statut "Projet".
  Un e-mail est envoyé au déclarant de l'incident.
- Le Risk Manager peut :
  - **Valider** l'incident qui prend le statut "Validé".
  - **Rejeter** l'incident.
- Quand un incident validé est considéré comme terminé, le Risk Manager peut **Fermer** l'incident, qui prend le statut "Fermé".

  ☛ *Voir aussi le diagramme de définition de workflow Workflow des incidents.*

Détail des étapes du processus de gestion des incidents

☛ *Pour visualiser le diagramme de définition de workflow des incidents, voir Workflow des incidents.*

Soumettre un incident

Une fois que vous avez saisi les informations concernant l'incident, vous pouvez le soumettre.

Pour soumettre un incident :

1. Voir Accéder aux incidents.
2. Sélectionnez l'incident que vous souhaitez traiter et cliquez sur **Workflow > Soumettre**.

Si l'entité du déclarant de l'incident a un "Approbateur d'incident", le statut de l'incident passe à "À approuver" et l'incident apparaît dans la liste des incidents à approuver par l'approbateur. Dans le cas contraire, le statut de l'incident passe à "À valider" et l'incident apparaît dans la liste des incidents à valider par le Risk Manager.

Approuver un incident

Après soumission de l'incident pour approbation, l'approbateur d'incident de l'entité du déclarant peut examiner, compléter si besoin et soumettre l'incident pour validation.

☛ *S'il n'y a pas d'approbateur d'incident sur l'entité, l'incident passe directement au stade de la validation. Voir Valider un incident.*

Pour approuver un incident :

1. Cliquez sur **Incidents**.
2. Sélectionnez l'incident à approuver et cliquez sur **Workflow**.
3. Sélectionnez l'une des transition suivantes :
   - **Approuver et soumettre** : le statut de l'incident passe à "À valider".
   - **Demander des modifications**
   - **Rejeter**

Valider un incident

Une fois les incidents renseignés avec leurs pertes, récupérations et provisions, vous pouvez les valider.

☛ *Seuls les Risk Managers sont autorisés à valider les incidents.*

Pour valider un incident :

1. Cliquez sur **Incidents**.
2. Dans la liste déroulante, sélectionnez **Incidents**.
   La liste des incidents dont vous avez la responsabilité apparaît.
3. Sélectionnez l'incident que vous souhaitez traiter et cliquez sur **Workflow**.
4. Sélectionnez l'une des transitions suivantes :
   - **Valider** : l'incident prend le statut "Validé"
   - **Demander des modifications**
   - **Rejeter**

Fermer un incident

Une fois l'incident validé, le Risk Manager peut décider que cet incident ne sera plus modifié et donc de le fermer.

☛ *Seuls les Risk Managers sont autorisés à fermer les incidents.*

Pour fermer un incident :

1. Cliquez sur **Incidents**
2. Dans la liste déroulante, sélectionnez **Incidents non clos**.
3. Sélectionnez l'incident que vous souhaitez fermer et cliquez sur **Workflow > Fermer**.

RAPPORTS CONCERNANT LES INCIDENTS

Les différents types de rapports proposés en standard par **Hopex LDC** visent à analyser et à suivre les incidents et de leurs conséquences financières. Tous les rapports sont présentés dans la devise locale de l'utilisateur si le taux de change entre la devise de référence et la devise locale est renseigné. Si le taux de change n'est pas renseignés, les rapports sont présentés dans la devise de références.

☛ *Pour plus de détails sur l'utilisation des rapports, voir le guide **Hopex Common Features**.*

☛ *Voir également : Rapports concernant les incidents.*

✓ Les rapports d'analyse des pertes
✓ Les rapports de Back Testing
✓ Les rapports de calcul de capital

☛ *Pour plus de détails sur les rapports, voir :*

- *Accéder aux rapports*
- *Créer un rapport*

LES RAPPORTS D'ANALYSE DES PERTES

Répartition des incidents et des pertes

Ce rapport permet de visualiser la répartition des incidents et des pertes sélectionnés selon plusieurs axes : par entité, par ligne métier, par type de risque, ou par processus.

☛ *Pour plus de détails sur la procédure qui permet de relier incident, ou une perte, à une entité ou à un processus, voir Définir le périmètre d'une perte.*

Chemin d'accès

Barre de navigation > Rapports

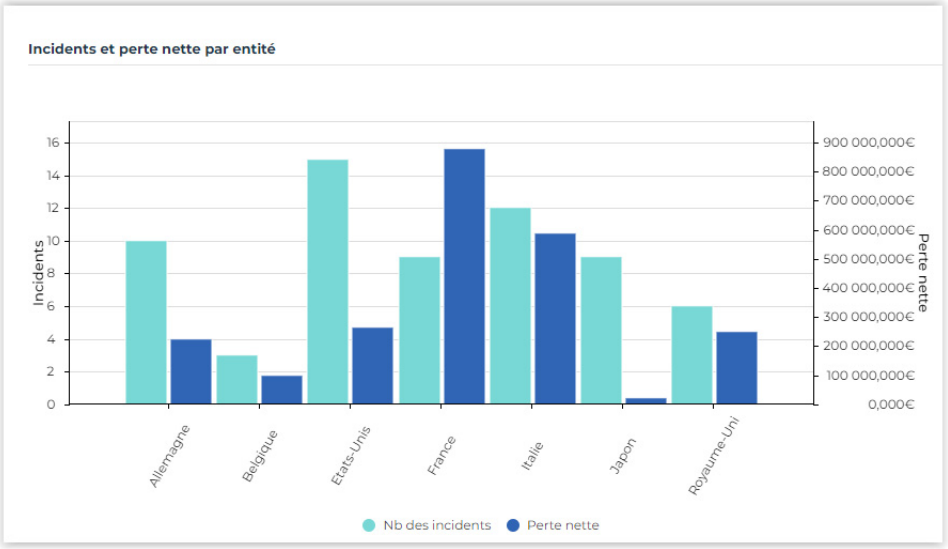
Paramètres du rapport

Il s'agit ici de sélectionner les incidents et les pertes qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les lignes métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Type de risque	***Type de risque***	Sélection des incidents reliés aux risques type de la liste ou à leurs sous risques type. Non obligatoire.
Processus	***Processus***	Sélection des incidents reliés aux processus de la liste ou à leurs sous-processus. Non obligatoire.

Paramètres	Type du paramètre	Contraintes
Catégorie de processus	***Catégorie de processus***	Sélection des incidents reliés aux processus de la liste ou à leurs sous-processus. Non obligatoire.
Entités	***Entité***	Sélection des incidents reliés aux entités de la liste ou à leurs sous-entités. Non obligatoire.
Lignes métier	***Lignes métier***	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Exemple



Evolution des incidents et des pertes par mois

Ce rapport permet de visualiser la répartition mensuelle des incidents et la répartition mensuelle des pertes sur deux diagrammes en bâton différents.

☛ *Pour plus de détails sur la procédure permettant de relier un incident à une perte, voir Saisir une perte.*

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

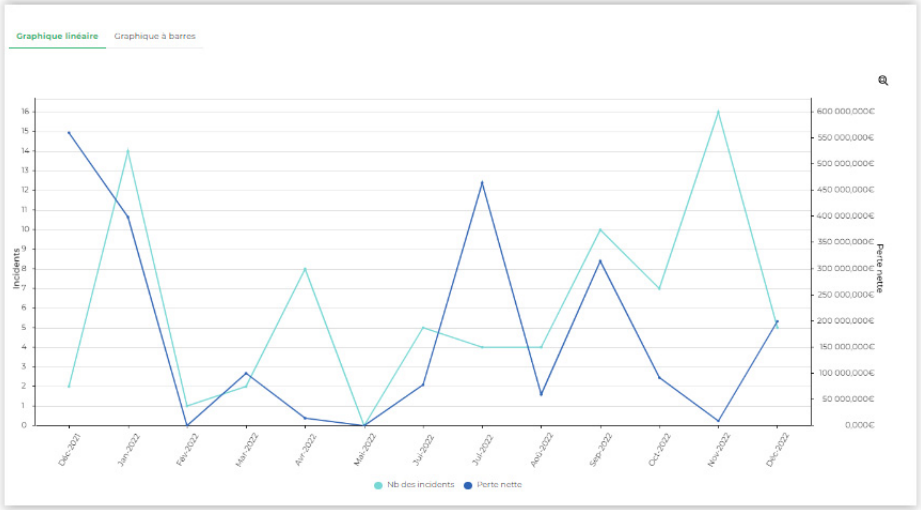
Il s'agit ici de sélectionner les incidents et les pertes qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les lignes métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Type de risque	Type de risque	Sélection des incidents reliés aux risques type de la liste ou à leurs sous risques type. Non obligatoire.
Processus organisationnel	Processus organisationnel	Sélection des incidents reliés aux processus de la liste ou à leurs sous-processus. Non obligatoire.
Catégorie de processus	Catégorie de processus	Sélection des incidents reliés aux catégories de processus de la liste ou aux sous-catégories. Non obligatoire.
Entités	Entité	Sélection des incidents reliés aux entités de la liste ou à leurs sous-entités. Non obligatoire.
Lignes métier	Lignes métier	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Résultats

Ce rapport affiche le nombre d'incidents et les pertes nettes correspondantes (somme des pertes - sommes des récupérations) par mois entre deux dates.

☛ *Si aucun paramètre n'est défini, tous les incidents sont pris en compte. Sinon, seuls les incidents reliés aux types d'objets spécifiés en paramètre et à leur fils (types de risque, processus métier, processus organisationnels, entités et lignes métier) sont affichés.*



Evolution des incidents et des pertes par type de risque

Ce rapport permet de visualiser les courbes d'évolution mensuelle des incidents et des pertes sur un même diagramme.

☛ *Pour plus de détails sur la procédure permettant de relier un incident à une perte, voir Saisir une perte.*

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les incidents et les pertes à présenter en précisant éventuellement les types de risque du périmètre.

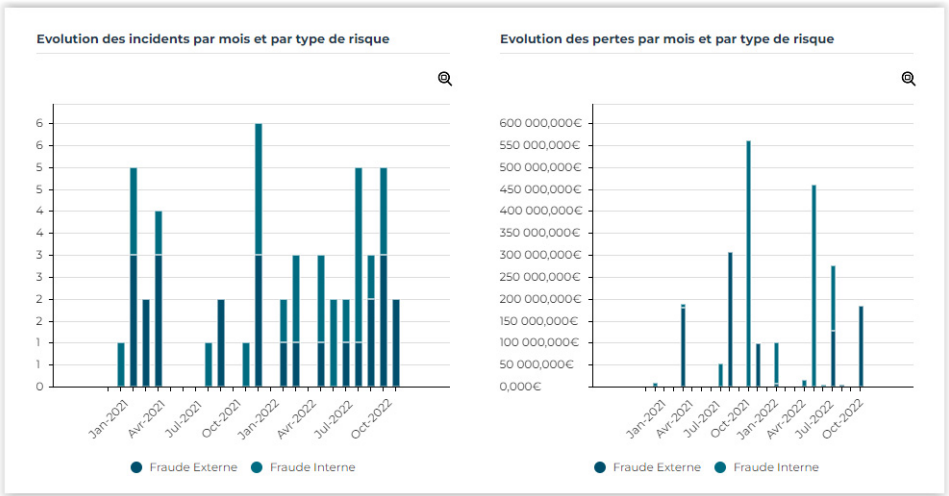
Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise de l'utilisateur est utilisée par défaut.
Seuil	Réel	Prend en compte les incidents dont le montant des pertes est supérieur à ce seuil.

Paramètres	Type du paramètre	Contraintes
Date de début	Date	Un an avant la date courante (par défaut)
Date de fin	Date	Date courante (par défaut)
Type de risque	Type de risque	Sélection des incidents reliés aux types de risque de la liste ou à leurs sous-types. Non obligatoire.

Résultats

Ce rapport se compose de deux chapitres :

- **Evolution des incidents** par mois et par type de risque :affiche le nombre d'incidents déclarés par mois, entre une date de début et une date de fin, et répartis par type de risque
- **Evolution des pertes** par mois et par type de risque : affiche les pertes nettes (somme des pertes - somme des récupérations) d'un ensemble d'incidents



☛ *Pour ces deux chapitres de rapport, si aucun type de risque n'est défini en paramètre, tous les incidents sont pris en compte. Sinon, seuls les incidents reliés aux types de risques sélectionnés et à leurs fils sont affichés.*

LES RAPPORTS DE BACK TESTING

Ces rapports permettent d'obtenir le montant des pertes financières des risques étudiés à partir des incidents qui leur sont attachés.

> ☛ *Pour plus de détails sur la procédure qui permet de relier un incident, ou une perte, à un type de risque, voir Définir le périmètre d'une perte.*

Les risques affichés dans les rapports sont les risques définis en paramètre ainsi que leurs sous-risques.

Pertes par risque (Back-testing)

Chemin d'accès

Barre de navigation > Rapports

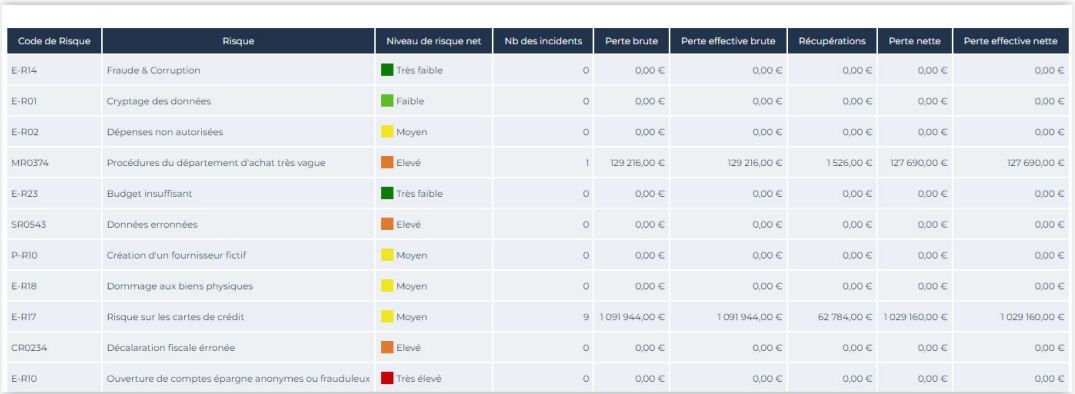
Paramètres du rapport

Il s'agit ici de sélectionner les risques qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les lignes métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil de perte nette d'incident	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Type de risque	***Type de risque***	Sélection des incidents reliés aux risques type de la liste ou à leurs sous risques type. Non obligatoire.
Processus	***Processus***	Sélection des incidents reliés aux processus de la liste ou à leurs sous-processus. Non obligatoire.

Paramètres	Type du paramètre	Contraintes
Catégorie de processus	***Catégorie de processus***	Sélection des incidents reliés aux catégories de processus de la liste ou aux sous-catégories. Non obligatoire.
Entités	***Entité***	Sélection des incidents reliés aux entités de la liste ou à leurs sous-entités. Non obligatoire.
Lignes métier	***Lignes métier***	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Résultat



Code de Risque	Risque	Niveau de risque net	Nb des incidents	Perte brute	Perte effective brute	Récupérations	Perte nette	Perte effective nette
E-R14	Fraude & Corruption	Très faible	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
E-R01	Cryptage des données	Faible	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
E-R02	Dépenses non autorisées	Moyen	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
MR0374	Procédures du département d'achat très vague	Elevé	1	129 216,00 €	129 216,00 €	1 526,00 €	127 690,00 €	127 690,00 €
E-R23	Budget insuffisant	Très faible	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
SR0543	Données erronnées	Elevé	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
P-R10	Création d'un fournisseur fictif	Moyen	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
E-R18	Dommage aux biens physiques	Moyen	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
E-R17	Risque sur les cartes de crédit	Moyen	9	1 091 944,00 €	1 091 944,00 €	62 784,00 €	1 029 160,00 €	1 029 160,00 €
CR0234	Décalaration fiscale érronée	Elevé	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
E-R10	Ouverture de comptes épargne anonymes ou frauduleux	Très élevé	0	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €

Incidents X Niveau de risque par type de risque (Back-testing)

Chemin d'accès

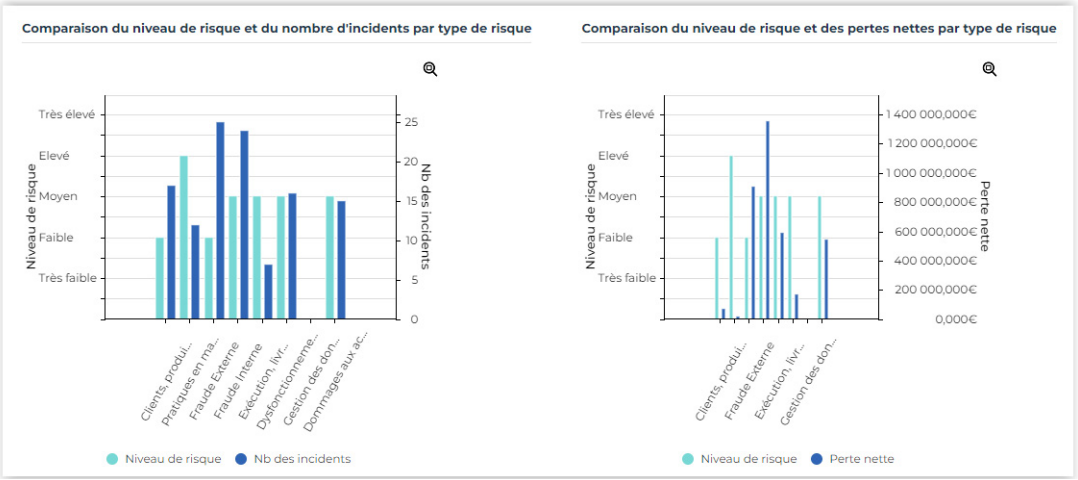
Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les types risques qui seront présentés dans le rapport.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil de perte nette d'incident	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Types de risque	***Type de risque***	Sélection des incidents reliés aux types de risque ou aux sous-types de risque. Non obligatoire.

Résultat



Incidents X Niveau de risque par ligne métier (Back-testing)

Il s'agit ici de sélectionner les lignes métier dont les risques seront présentés dans le rapport.

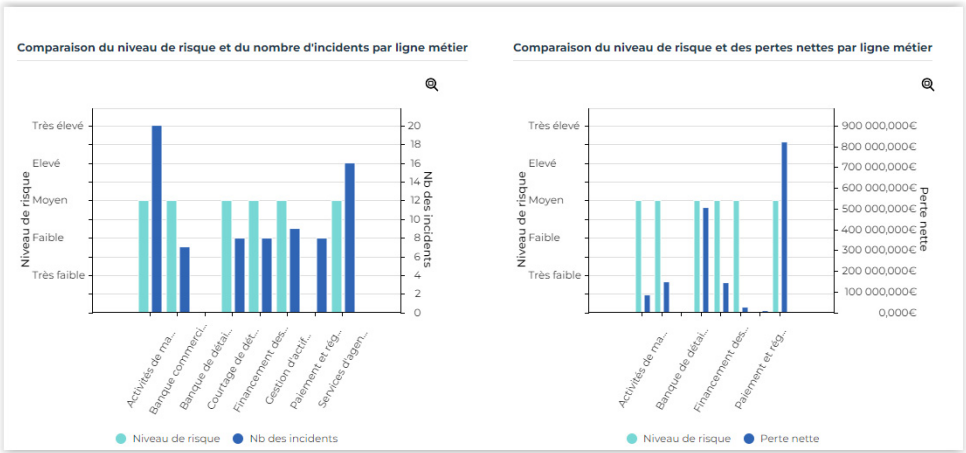
Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Lignes métier	***Lignes métier***	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Résultat



LES RAPPORTS DE CALCUL DE CAPITAL

Ces rapports sont utilisés pour évaluer le montant du capital à provisionner pour couvrir les risques opérationnels.

Matrice de distribution des pertes

Ce rapport permet d'obtenir la répartition des pertes en fonction des lignes métier (présentées en colonne) et des types de risque (présentés en ligne).

Pour chaque couple (ligne métier, type de risque), ce rapport présente :

- Le montant total des pertes,
- Le montant minimum des pertes,
- Le montant maximum des pertes,
- Le nombre d'incidents.

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les incidents et les pertes qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les lignes métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil de perte nette	Réel	Montant minimum des pertes affichées.
Année d'analyse	Entier	Année précédent l'année courante par défaut.
Type de risque	Type de risque	Sélection des incidents reliés aux risques type de la liste ou à leurs sous risques type. Non obligatoire.
Lignes métier	Lignes métier	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Résultat

		Aéroport	Banque	Industrie
Clients, produits et pratiques commerciales	Perte totale	-	60 356,00 €	-
	Perte maximum	-	18 872,00 €	-
	Perte Min	-	0,00 €	-
	Nb des incidents	0	16	0
Dommages aux actifs corporels	Perte totale	9 847,00 €	504 205,00 €	29 521,00 €
	Perte maximum	7 967,00 €	250 000,00 €	25 433,00 €
	Perte Min	0,00 €	0,00 €	4 088,00 €
	Nb des incidents	3	10	2
Dysfonctionnement de l'activité et des systèmes	Perte totale	12 289,00 €	154 620,00 €	3 000,00 €
	Perte maximum	12 289,00 €	56 064,00 €	3 000,00 €
	Perte Min	12 289,00 €	0,00 €	3 000,00 €
	Nb des incidents	1	14	1
Exécution, livraison et gestion des processus	Perte totale	-	591 460,00 €	-
	Perte maximum	-	395 400,00 €	-
	Perte Min	-	0,00 €	-
	Nb des incidents	0	7	0

Approche de l'indicateur de base (BIA)

Ce rapport permet d'obtenir une estimation du montant du capital à allouer pour une ligne métier. Pour chaque année de la période définie par les paramètres, le rapport présente :

- Le total des revenus bruts, par année

  ☛ *Pour créer des revenus, voir Saisir les revenus bruts pour la gestion des incidents.*

- Le revenu brut moyen sur le nombre d'années spécifié en paramètre
- Le taux BIA défini en paramètre
- Le montant du capital à allouer pour la ligne métier (pourcentage de BIA appliqué au revenu brut moyen).

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les incidents et les pertes qui seront présentés en précisant les éléments qui définissent leur périmètre. Dans le cas de ce rapport, le périmètre est défini par une seule ligne métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil de revenu brut	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Période moyenne	Entier	Nombre d'années sur lequel porte le calcul de la moyenne.
Pourcentage de BIA	Réel	Valeur du pourcentage à appliquer.
Ligne métier	Ligne métier	Obligatoire.

Résultat

	2014	2015	2016	2017	2018	2019
Produit brut	0,00 €	66 000 000,00 €	76 000 000,00 €	67 000 000,00 €	68 000 000,00 €	-
Produit brut moyen	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%
Allocation de capital	-	3 300 000,00 €	7 100 000,00 €	7 150 000,00 €	6 750 000,00 €	3 400 000,00 €

Approche standard (TSA)

Ce rapport, issue de Bâle II, permet d'obtenir une estimation du montant du capital à allouer par ligne métier.

Pour chaque ligne métier, le rapport présente :

- Le total des revenus bruts, par année
- Le revenu brut moyen sur le nombre d'années spécifié en paramètre
- Le taux TSA retenu pour la ligne métier
- Le montant du capital à allouer pour la ligne métier (pourcentage de TSA appliqué au revenu brut moyen).

Chemin d'accès

Barre de navigation > Rapports

Paramètres du rapport

Il s'agit ici de sélectionner les incidents et les pertes qui seront présentés en précisant les éléments qui définissent leur périmètre : les types de risque, les entités, les processus ou les lignes métier.

Paramètres	Type du paramètre	Contraintes
Devise	Devise	Devise des rapports. La devise locale est utilisée par défaut.
Seuil de revenu brut	Réel	Montant minimum des pertes affichées.
Date de début	Date	Un an avant la date courante par défaut.
Date de fin	Date	Date courante par défaut.
Période moyenne	Entier	Nombre d'années sur lequel porte le calcul de la moyenne.
Lignes métier	Lignes métier	Sélection des incidents reliés aux lignes métier de la liste ou à leurs sous-lignes métier. Non obligatoire.

Résultat

	% TSA	Sous-menu	2015	2016	2017	2018	2019
Banque	12.0%	Produit brut	66 000 000,00 €	76 000 000,00 €	67 000 000,00 €	68 000 000,00 €	-
		Produit brut moyen	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%
		Allocation de capital	-	8 520 000,00 €	8 580 000,00 €	8 100 000,00 €	4 080 000,00 €
Banque commerciale	15.0%	Produit brut	0,00 €	0,00 €	0,00 €	0,00 €	-
		Produit brut moyen	N/A	0,00 €	0,00 €	0,00 €	0,00 €
		% TSA	-	15.0%	15.0%	15.0%	15.0%
		Allocation de capital	-	0,00 €	0,00 €	0,00 €	0,00 €
Gestion d'actifs	11.0%	Produit brut	0,00 €	0,00 €	0,00 €	0,00 €	-
		Produit brut moyen	N/A	0,00 €	0,00 €	0,00 €	0,00 €
		% TSA	-	11.0%	11.0%	11.0%	11.0%
		Allocation de capital	-	0,00 €	0,00 €	0,00 €	0,00 €
Services d'agence	13.0%	Produit brut	0,00 €	0,00 €	0,00 €	0,00 €	-
		Produit brut moyen	N/A	0,00 €	0,00 €	0,00 €	0,00 €
		% TSA	-	13.0%	13.0%	13.0%	13.0%
		Allocation de capital	-	0,00 €	0,00 €	0,00 €	0,00 €

HOPEX Cyber Resilience

Guide d’utilisation

HOPEX Aquila

MEGA
SEE THE BIGGER PICTURE

SOMMAIRE

Sommaire

INTRODUCTION À HOPEX CYBER RESILIENCE

Voir aussi :

- Étapes du processus de cyber-résilience
- Les fournisseurs TIC
- Les risques TIC
- Rapports de cyber-résilience

Définition de la cyber-résilience

La cyber-résilience est la capacité d'une entité à garantir son intégrité et à mettre en place des mesures préventives contre les cyberattaques. Il s'agit d'une approche large qui englobe la cybersécurité et le Management de la Continuité d'Activité.

Contexte

Hopex Cyber Resilience est un module qui permet de mettre en place des stratégies de résilience. Il permet de se conformer aux réglementations concernant les évaluations de risques TIC et aux standards de cyber-résilience, tels que :

- DORA (UE) : applicable dès janvier 2025 à toutes les entreprises ayant une activité au sein de l'Union Européenne.
- CSF (NIST, USA)
- PRA Operational Resilience (BoE, UK)
- Sound Practices to Strengthen Operational Resilience (OCC, USA)
- CPS 234 (APRA, Australie)
- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI, Inde)

Utilisation avec d'autres solutions

Hopex Cyber Resilience doit être utilisé conjointement avec :

- **Hopex BCM**
- **Hopex GRC**
- **Hopex IT Portfolio Management**

☛ *Il peut également être utilisé avec le framework UCF pour accélérer votre initiative de cyberconformité (voir A propos de "Unified Compliance Framework").*

Installation du module Cyber Resilience (CYRES)

Prérequis :

Vous devez avoir installé au préalable le module "ITPM Excel Import Template".

☛ *Pour plus de détails sur l'installation des modules, voir Importer un module dans HOPEX.*

DÉVELOPPER VOTRE CYBER-RÉSILIENCE

- ✓ Étapes du processus de cyber-résilience
- ✓ Les fournisseurs TIC
- ✓ Les risques TIC
- ✓ Rapports de cyber-résilience

ÉTAPES DU PROCESSUS DE CYBER-RÉSILIENCE

Hopex Cyber Resilience vous accompagne tout au long de votre initative de cyber-résilience.

Voir aussi :

- Introduction à Hopex Cyber Resilience
- Les fournisseurs TIC
- Les risques TIC
- Rapports de cyber-résilience

Gérer l'environnement informatique

Types d'objets gérés par les solutions GRC

Les solutions GRC permettent de gérer :

- les processus de l'entreprise
  - ☛ *Voir Gérer les catégories de processus et processus.*
- les ressources informatiques associées
  - ☛ *Voir Gérer les applications.*
- les risques liés aux TIC
  - ☛ *Voir Gérer les risques.*

Types d'objets gérés par Hopex Cyber Resilience

Hopex Cyber Resilience permet de visualiser les types d'objet suivants :

- Technologie

  Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.

  *Pour y accéder, cliquez sur **Environnement > Organisation > Technologies**.*

- Centre de données

  Un centre de données est un site physique qui regroupe des installations informatiques chargées de stocker et de distribuer des données à travers un réseau interne ou via un accès Internet.

- Installation

  Une installation est un modèle de site d'intérêt pour l'entreprise (par exemple : une usine ou une agence).

- Serveur (déployé)

  Un serveur (déployé) est une ressource informatique sur laquelle des applications s'exécutent.

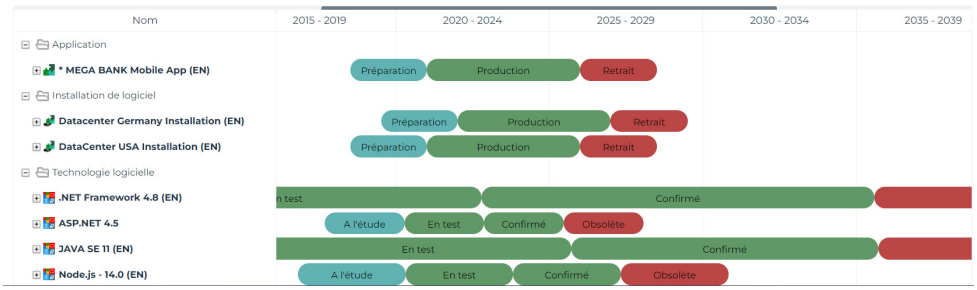
- Catégorie de données

  Une catégorie de données représente un type de données ayant des caractéristiques communes (par exemple : données sensibles, données confidentielles).

Bilans d'Impacts sur l'Activité et ***Plans de Continuité d'Activité*** peuvent être visualisés dans les propriétés des types d'objet suivants :

- technologies
- centres de données
- installations
- serveurs déployés

Un ***diagramme de Gantt*** peut être visualisé dans les propriétés des applications et technologies logicielles :



Excel pour la construction de l'environnement de résilience

Un modèle Excel permet d'accélérer la création d'objets nécessaires à la mise en place d'une initiative de cyber résilience.

Pour plus de détails sur les modèles Excel, voir la documentation Fonctionnalités communes sur Excel.

Modules complémentaires à Hopex Cyber Resilience

Le module **Hopex Cyber Resilience** peut être utilisé conjointement avec :

- ITMC Discovery, pour découvrir de manière automatisée les technologies et applications d'une entreprise installées on-premise.

  ☛ *Voir Inventorier les technologies avec ITMC Discovery*

- **AI-Driven APM** (APM piloté par l'IA), pour distinguer les technologies des applications

  ☛ *Voir Distinguer les applications des technologies.*

- **ServiceNow Integration**, pour synchroniser des objets entre **Hopex** et ServiceNow.

  ☛ *Voir ServiceNow Integration.*

Identifier les processus et ressources informatiques critiques

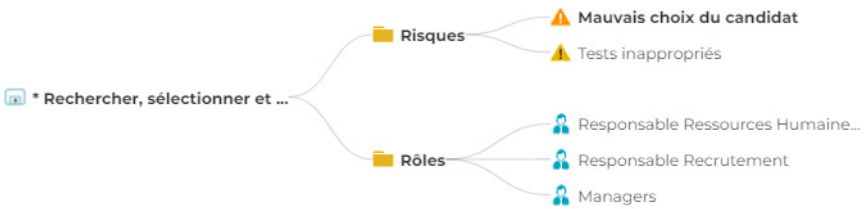
Les risques liés aux technologies de l'information et de la communication (TIC) doivent être identifiés.

Vous devez procéder à des Bilans d'Impact sur l'Activité (BIA) pour identifier les processus et ressources critiques.

☛ *Voir Définir un Bilan d'Impact sur l'Activité.*

Le rapport **Impacts de BIA**, qui se présente sous forme d'un dendrogramme, affiche les risques, applications et technologies. Vous pouvez cliquer sur les éléments du dendrogramme pour déplier le rapport.

Lorsque vous passez la souris sur un objet, vous pouvez visualiser des valeurs le concernant dans un info-bulle.



☛ *Ce rapport est disponible dans la page **Rapports** des propriétés d'un BIA (**Continuité > Bilans d'Impact sur l'Activité**).*

Évaluer le framework de cyber-résilience

Les cyber-risques doivent être évalués. Un modèle de questionnaire spécifique est disponible.

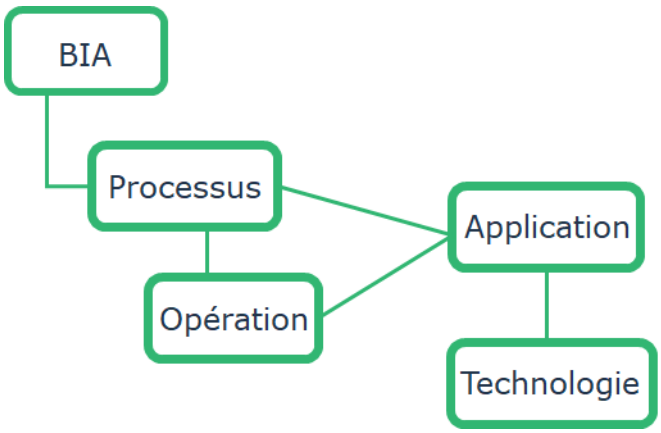
☛ *Voir Les risques TIC.*

Planifier la stratégie de cyber-résilience

Vous devez documenter et tester les Plans de Continuité d'Activité.

☛ *Voir Concevoir un Plan de Continuité d'Activité et Tester un Plan de Continuité d'Activité.*

Dans les propriétés des applications et technologies logicielles reliées aux processus critiques, vous pouvez visualiser les BIA et PCA concernés.



Gérer les cyberincidents

Vous devez documenter, notifier et suivre les cyberincidents.

☛ *Pour des informations générales sur les incidents, voir Collecte des incidents.*

Causes d'un incident et type d'incident

Dans les propriétés d'un incident, la section **Analyse quantitative** permet de :

- saisir la **Description des causes** de l'incident.
- sélectionner le **Type d'incident**.

📖 *Le Type d'incident correspond au type de risque matérialisé.*

Incident majeur

Un incident peut être considéré comme **Majeur** (case à cocher dans la page **Caractéristiques** des propriétés de l'incident).

📖 *Un incident est dit majeur lorsqu'il a un fort impact négatif sur des fonctions importantes ou critiques de l'organisation.*

Cette caractéristique est utile pour pouvoir générer le rapport MS Word d'incidents majeurs. Voir Rapport (MS-Word) des incidents majeurs.

Calcul du temps écoulé depuis la détection d'un incident

Une caractéristique calculée permet d'afficher le nombre de jours/heures écoulés depuis la date de détection de l'incident.

Cette caractéristique calculée est affichée :

- dans la page **Caractéristiques** des propriétés des incidents
- en colonne, dans la liste d'incidents accessible via le menu **Incidents**
- dans le rapport MS Word des incidents majeurs
- dans la page **Incidents** des propriétés des types d'objet suivants :
  - risques
  - catégories de processus
  - processus
  - macro-incidents
  - acteurs
  - applications
  - lignes métier
  - produits

Rapports concernant les incidents

Des rapports spécifiques permettent de :

- générer un rapport des incidents majeurs pour informer les autorités.

  ☛ *Voir Rapport (MS-Word) des incidents majeurs.*

- analyser les incidents.

  ☛ *Voir Analyse nœud papillon d'un incident.*

- surveiller les cyberincidents qui surviennent.

  ☛ *Voir Surveillance des incidents.*

Visualiser les PCA déclenchés suite à un incident

Dans les propriétés d'un incident, une page **Gestion de crises** vous donne des informations sur les PCA déclenchés.

☛ *Cette page est disponible si au moins un PCA déclenché est relié à l'incident.*

Piloter la cyber-résilience

Des rapports vous permettent de piloter votre initiative de cyber-résilience.

Pour plus de détails, voir Rapports de cyber-résilience.

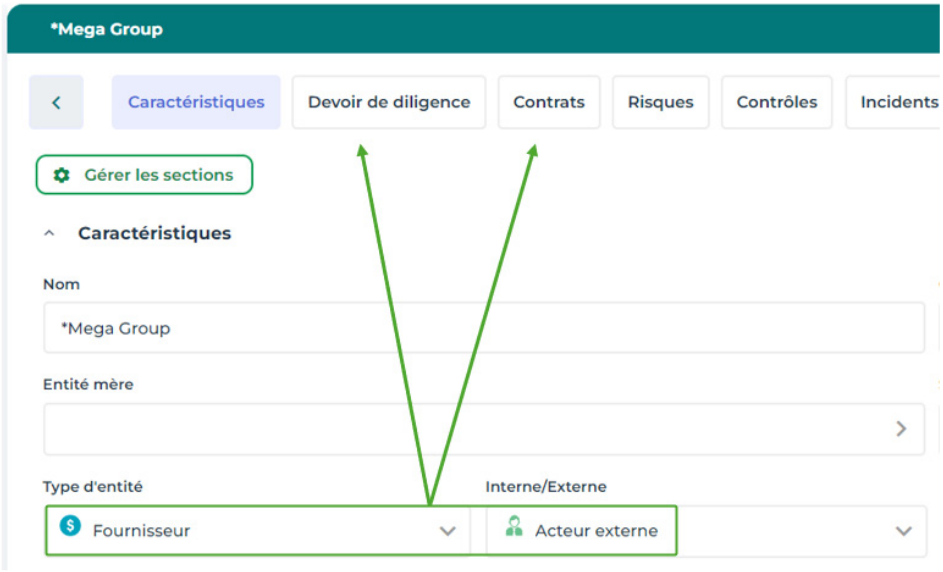
LES FOURNISSEURS TIC

Un fournisseur TIC est une entreprise qui fournit des services TIC (Technologies de l'Information et de la Communication).

Dans **Hopex**, un fournisseur (ou prestataire) est une acteur ***externe*** de type ***fournisseur***.

Lorsque l'entité est un acteur ***externe*** de type "***Fournisseur***", vous pouvez :

- procéder à une évaluation du fournisseur avec la diligence requise.
- spécifie les contrats concernant ce fournisseur



Accéder aux fournisseurs TIC

Pour accéder aux fournisseurs TIC :

1. Dans la barre de navigation, sélectionnez **Environnement > Organisation > Fournisseurs**.

   ☛ *Une hiérarchie de fournisseurs est également disponible via **Processus > Par entité > Fournisseurs**.*

   Le dossier "Fournisseurs" est disponible s'il existe au moins un fournisseur dans le référentiel.

Créer un fournisseur TIC

Pour créer un fournisseur TIC :

1. Voir Accéder aux fournisseurs TIC.
2. Cliquez sur **Nouveau**.
   Le fournisseur est créé automatiquement.

   ☛ *Dans les propriétés du fournisseur, vous pouvez remarquer qu'il s'agit d'un acteur externe de type Fournisseur.*

Spécifier les contrats des fournisseurs

Accéder aux contrats

Pour accéder aux contrats :

- Dans la barre de navigation, sélectionnez **Environnement > Organisation > Fournisseurs et contrats**.
  Vous pouvez, via des listes spécifiques, accéder :
  - à tous les **Contrats**
  - aux **Contrats par fournisseur**

Pour accéder aux contrats d'un fournisseur TIC :

1. Dans la barre de navigation, sélectionnez **Environnement > Organisation > Fournisseurs et contrats > Contrats par fournisseur.**
2. Dans la fenêtre de propriétés d'un fournisseur, sélectionnez la page **Contrats**.

Créer un contrat

Pour créer un contrat :

1. Dans la barre de navigation, sélectionnez **Environnement > Organisation > Fournisseurs et contrats > Contrats.**
2. Cliquez sur **Nouveau**.
3. (optionnel) Saisissez :
   - la **Date de début**
   - la **Date de fin**
   - le **Code**
   - le **Type du contrat**
   - un **Fournisseur**
4. Cliquez sur **OK**.

Visualiser le statut du contrat

Une fois créé, le contrat dispose d'un **Statut**, calculé automatiquement:

- **Signé**

  ☛ *Le contrat est considéré "signé" lorsque la date du jour est antérieure à la date de début du contrat.*

- **En vigueur**

  ☛ *Le contrat est considéré "En vigueur" lorsque la date du jour se trouve dans l'intervalle de temps compris entre la date de début du contrat et sa date de fin.*

- **Expiré**

  ☛ *Le statut est considéré "Expiré" lorsque la date du jour est postérieure à la date de fin du contrat.*

- **Non connu**

  ☛ *Le statut est considéré "Non connu" lorsque les dates n'ont pas été renseignées.*

Spécifier les caractéristiques du contrat

Dans les propriétés du contrat vous pouvez éventuellement spécifier :

- le **Type de contrat**
- le **Fournisseur** concerné par le contrat
- l'entité **Signataire**
- les **Éléments du contrat**
  Vous pouvez relier les objets qui font l'objet du contrat :
  - Application

    🕮 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

  - Technologie logicielle

    🕮 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

  - Processus

    🕮 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

  - Opération

    🕮 *Une opération est une étape élémentaire d'un processus. Elle correspond à l'intervention d'un acteur de l'organisation.*

  - Serveur

    🕮 *Un serveur (déployé) est une ressource informatique sur laquelle des applications s'exécutent.*

  - Site

    🕮 *Un site est un lieu géographique où est implantée l'entreprise. Les sites peuvent être des sites-types tels que le siège, l'agence, l'usine, ou*

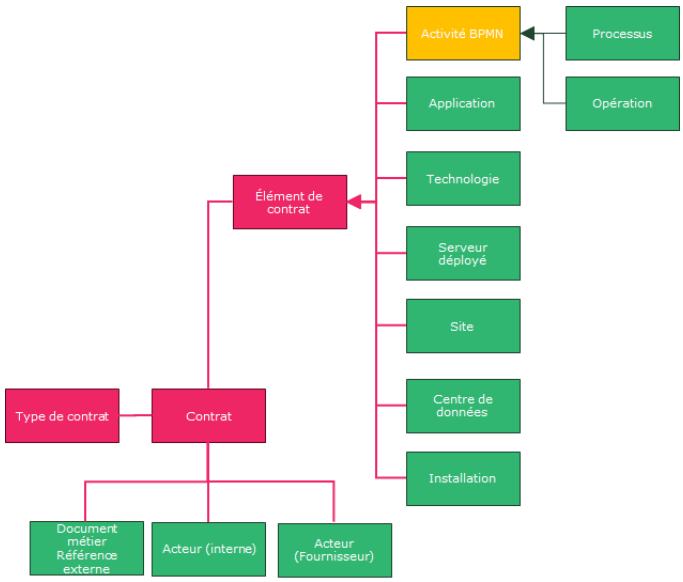
des lieux géographiques précis comme l'agence de Marseille, l'usine de Poissy, etc.

- Centre de données

  Un centre de données est un site physique qui regroupe des installations informatiques chargées de stocker et de distribuer des données à travers un réseau interne ou via un accès Internet.

- Installation

  Une installation est un modèle de site d'intérêt pour l'entreprise (par exemple : une usine ou une agence).



Pièces jointes

Dans la section **Pièces jointes** vous pouvez joindre le contrat.

Pour plus d'information sur les documents métier, voir Utiliser les documents métier.

Évaluer les fournisseurs TIC

Évaluer unitairement un fournisseur TIC

Pour évaluer unitairement un fournisseur TIC :

1. Dans les propriétés d'un fournisseur, sélectionnez la page **Devoir de diligence**.
2. Cliquez sur **Nouvelle évaluation**.
3. Modifiez éventuellement la **Date**.

4. Spécifiez si le fournisseur est :
   - **Conforme**

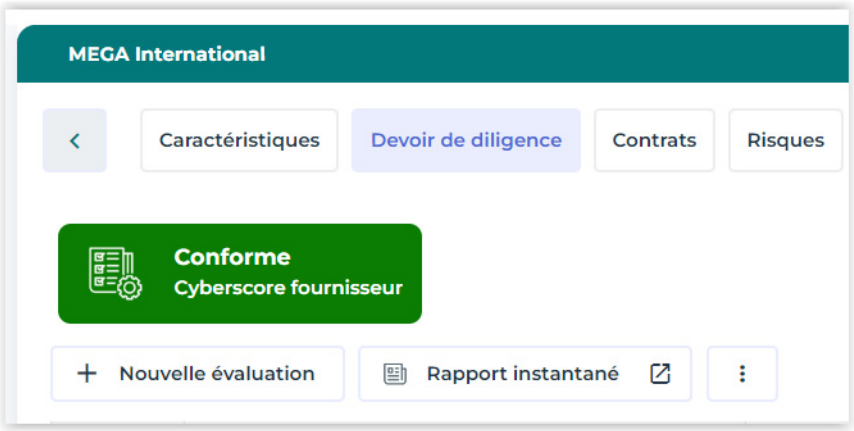
     ☛ *Un fournisseur dit "conforme" est un fournisseur conforme aux exigences de cybersécurité. Il peut être considéré comme un partenaire privilégié, fiable et sûr.*
   - **Potentiel**

     ☛ *Un fournisseur dit "potentiel" a passé le processus de diligence avec succès mais doit s'améliorer ou être surveillé pour remplir complètement les exigences de cybersécurité. Il peut être considéré comme un partenaire prometteur, mais doit fournir des efforts supplémentaires pour s'améliorer en matière de cybersécurité.*
   - **Critique**

     ☛ *Un fournisseur dit "critique" présente des vulnérabilités ou risques importants en matière de cybersécurité. Il peut être considéré pour certains types de services ou collaborations à condition que des mesures d'atténuation appropriées soient mises en œuvre. Une attention et une surveillance particulières sont exigées en raison des risques sous-jacents.*
   - **Non conforme**

     ☛ *Un fournisseur dit "non conforme" ne remplit pas les exigences minimales de cybersécurité et représente un risque élevé pour la sécurité des données et opérations. Il peut s'avérer nécessaire de l'éviter ou de mettre un terme à la collaboration avec ce fournisseur en raison du risque élevé de non-conformité et de l'atteinte potentielle à la sécurité globale de l'organisation.*
5. Cliquez sur **OK**.
   La notation du fournisseur apparaît. Toutes les évaluations apparaissent sous forme de liste.

Le dernier **Cyberscore fournisseur** apparaît en haut de la page.



Évaluer simultanément plusieurs fournisseurs TIC

Pour évaluer de manière simultanée plusieurs fournisseurs TIC :

1. Dans le menu de navigation, cliquez sur **Évaluation > Évaluation directe > Diligence multiple**.
2. Cliquez sur **Nouvelle évaluation**.

3. Sélectionnez un fournisseur dans l'arborescence qui apparaît et cliquez sur **OK**.
4. Cliquez sur chaque fournisseur (contexte) et évaluez le **Cyberscore fournisseur**.
5. Cliquez sur **Soumettre**.

Évaluer les fournisseurs TIC via des campagnes

Vous pouvez également évaluer les fournisseurs TIC via des campagnes d'évaluation.

Un modèle d'évaluation "Devoir de diligence" est disponible.

Pour lancer une campagne d'évaluation, voir Lancer une campagne d'évaluation

LES RISQUES TIC

Hopex Cyber Resilience vous permet de lancer des évaluations de risques concernant des actifs TIC dans un périmètre défini.

☛ *Pour une présentation générale de la fonctionnalité d'évaluation de risques, voir :*

- *Évaluer les risques*
- *Campagnes d'évaluation*

Cette section concerne les spécificités de l'évaluation des risques TIC.

Modèle d'évaluation pour les risques TIC

Contextes

Hopex Cyber Resilience propose un modèle d'évaluation des risques TIC avec pour contextes les types d'objets suivants :

- Entité

  🕮 *Une entité représente une personne ou un groupe de personnes qui interviennent dans les processus ou dans le système d'information de l'entreprise.*

- Catégorie de processus

  🕮 *Une catégorie de processus regroupe plusieurs processus. Elle permet de hiérarchiser les processus et d'accéder au niveau le plus fin de granularité des processus.*

- Processus

  🕮 *Un processus décrit la marche à suivre pour mettre en œuvre tout ou partie du processus d'élaboration d'un produit ou un flux.*

- Opération

  🕮 *Une opération est une étape élémentaire d'un processus. Elle correspond à l'intervention d'un acteur de l'organisation.*

  ☛ *Les risques sur les processus et opérations sont récupérés uniquement si ces processus et opérations sont reliés à un contrat en vigueur.*

- Site

  ☛ *Un site est un lieu géographique où est implantée l'entreprise. Les sites peuvent être des sites-types tels que le siège, l'agence, l'usine, ou*

des lieux géographiques précis comme l'agence de Marseille, l'usine de Poissy, etc.

- Application

  📖 *Une application est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques.*

- Technologie logicielle

  📖 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

- Serveur déployé

  📖 *Un serveur (déployé) est une ressource informatique sur laquelle des applications s'exécutent.*

- Centre de données

  📖 *Un centre de données est un site physique qui regroupe des installations informatiques chargées de stocker et de distribuer des données à travers un réseau interne ou via un accès Internet.*

- Installation

  📖 *Une installation est un modèle de site d'intérêt pour l'entreprise (par exemple : une usine ou une agence).*

- Contrat

  📖 *Un contrat est un accord entre l'organisation et un fournisseur.*

- Fournisseur

  ☛ *Un fournisseur est un acteur externe de type "Fournisseur".*

Répondants

Les répondants sont définis comme suit :

Type d'objet contexte	Responsabilité (rôle métier)
Technologie	Correspondant local de technologie
Application	Propriétaire local d'application, responsable informatique
Processus	Correspondant Risque
Catégorie de processus	Correspondant Risque
Entité / Fournisseur	Correspondant Risque, Risk Manager

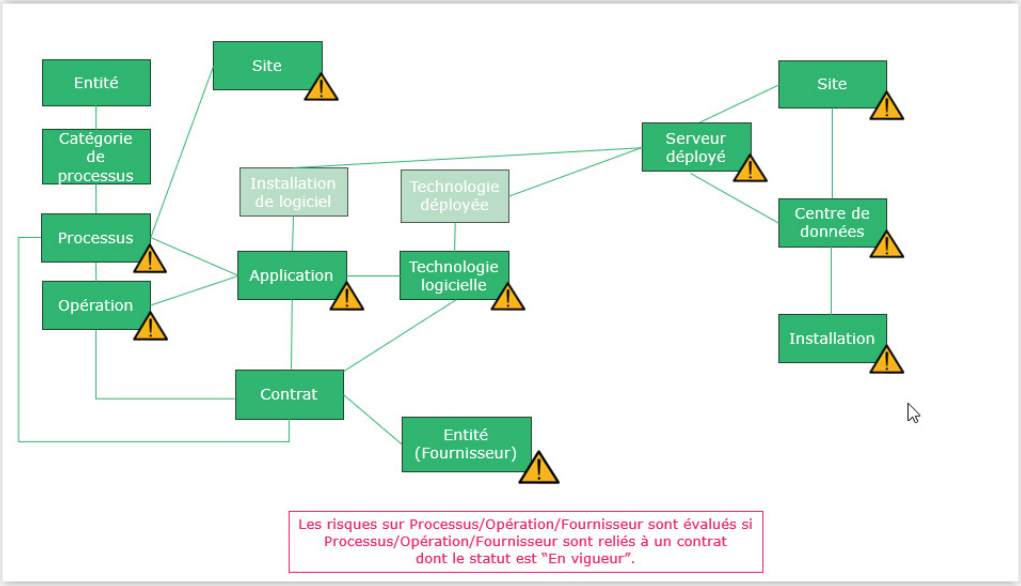
Rendu du questionnaire

Le questionnaire se présente sous forme de cartographie (heatmap ou carte de chaleur).

☛ *Pour plus de détails, voir Utiliser les questionnaires de type heatmap (cartographie).*

Pré-requis à l'évaluation des risques TIC

Pour pouvoir évaluer les fournisseurs TIC, vous devez avoir relié correctement les objets de votre environnement entre eux.



Lancer une évaluation de risques TIC

Vous pouvez évaluer plusieurs risques simultanément via une ***cartographie (heatmap) interactive***.

Pour évaluer simultanément plusieurs cyber-risques:

1. Dans la barre de navigation, cliquez sur **Évaluation > Évaluation directe > Évaluation multiple des risques**.
2. Cliquez sur **Nouvelle évaluation**.
3. Dans la fenêtre qui apparaît, sélectionnez le **Modèle d'évaluation "Évaluation des risques TIC".**
4. Dans l'arborescence affichée, sélectionnez l'entité contexte de l'évaluation.
5. Dépliez l'arborescence de manière à trouver les processus et applications.

   ☛ *Un risque est évalué dans le contexte des éléments de la branche qui remonte du risque jusqu'à la racine.*
6. Pour la suite de la procédure, voir Évaluer plusieurs risques simultanément.

   ☛ *Les risques TIC peuvent également être évalués via des campagnes d'évaluation. Voir Campagnes d'évaluation pour plus de détails.*

RAPPORTS DE CYBER-RÉSILIENCE

- ✓ Contrats et fournisseurs de services TIC
- ✓ Gantt des contrats de fournisseurs de services TIC
- ✓ Rapport (MS Word) des contrats fournisseurs
- ✓ Surveillance des incidents
- ✓ Impacts d'un incident
- ✓ Rapport (MS-Word) des incidents majeurs
- ✓ Analyse nœud papillon d'un incident
- ✓ Impacts d'un processus
- ✓ Vue d'ensemble des impacts TIC des processus
- ✓ Tableau de bord des risques par type de risque
- ✓ Tableau d'ensemble de criticité des processus et des actifs TIC de support
- ✓ Vue d'ensemble des fournisseurs par processus
- ✓ Actifs TIC critiques (à partir de Processus/Entité)

CONTRATS ET FOURNISSEURS DE SERVICES TIC

Ce rapport fournit une vision globale des contrats signés avec des fournisseurs TIC dans un laps de temps spécifique.

☛ *Pour plus de détails, voir Les fournisseurs TIC.*

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez éventuellement les filtres pour trouver le rapport **Contrats et fournisseurs de services TIC**.

Illustration

Tableau / Matrice

Paramètres du rapport

Paramètres
Date de début
Date de fin

Contenu du rapport

Ce rapport se présente sous forme de tableau et contient les colonnes suivantes :

- Nom du contrat
- Fournisseur
- Cyberscore

  ☛ *Voir Spécifier les contrats des fournisseurs.*
- Type de contrat
- Code
- Ressource
- Type de ressource
- Date de début
- Date de fin
- Statut
- Pièce jointes
- 1ère année (oui/non)

  ☛ *Les fournisseurs dont le contrat date de moins d'un an méritent un attention particulière.*

Exemple de rapport

Nom du contrat	Fournisseur	Cyber Rating	Type de contrat	Code	Ressource	Type de ressource	Date de début	Date de fin	Statut	Pièces jointes	1ère année
Contrat Amazon	Amazon.com (EN)		Achat de logiciel	CR001	Amazon Athena (EN)	Technologie logicielle	31/03/2024	30/11/2024	Signé	0	Non
Contrat Microsoft - 1	Microsoft		Achat de logiciel	Mic001	Azure Active Directory (EN)	Technologie logicielle	30/03/2024	30/04/2024	Signé	0	Non
Contrat Microsoft - 2	Microsoft		Achat de logiciel	Mic002	Azure Automation (EN)	Technologie logicielle	01/10/2023	03/03/2024	En vigueur	0	Non

GANTT DES CONTRATS DE FOURNISSEURS DE SERVICES TIC

Ce rapport représente un diagramme de Gantt des contrats signés avec les fournisseurs de TIC durant une période donnée.

Il affiche le cycle de vie des contrats, par fournisseur.

☛ *Pour plus de détails, voir Les fournisseurs TIC.*

Chemin d'accès

Vous pouvez générer ce rapport :

- individuellement, dans la page **Contrats** des propriétés d'un fournisseur (acteur externe de type "fournisseur").
- globalement, pour plusieurs fournisseurs (à partir du menu **Rapports** de la barre de navigation).

Illustration

Diagramme de Gantt

Paramètres du rapport

Lorsque vous générez ce rapport depuis le menu **Rapports** de la barre de navigation, les paramètres suivants sont disponibles :

Paramètres	Valeurs possibles
Date de début du contrat	
Date de fin du contrat	
Fournisseurs	
Cyberscore fournisseur	Conforme, potentiel, critique, Non conforme
Type de contrat	

Exemple de rapport

RAPPORT (MS WORD) DES CONTRATS FOURNISSEURS

Vous pouvez générer un rapport Word récapitulant les informations concernant les fournisseurs et contrats.

Chemin d'accès

Le rapport MS-Word des contrats fournisseurs peut être créé :

- à partir d'un fournisseur
- à partir d'une liste de fournisseurs

Pour générer le rapport à partir d'une liste de fournisseurs:

1. Voir Accéder aux fournisseurs TIC.
2. Sélectionnez un ou plusieurs fournisseurs.
3. Cliquez sur ⋮ et sélectionnez **Documentation > Rapport des Contrats fournisseurs**.
   Le rapport se génère.

Illustration

Rapport MS-Word

Paramètres du rapport

Les deux dates à saisir en paramètre permettent de définir un intervalle de temps durant lequel les contrats débutent.

Fournisseurs	
Date de début (Min)	Inclut les contrats débutant à cette date
Date de début (Max)	Inclut les contrats débutant à cette date (au plus tard)

Contenu du rapport

Le rapport contient les informations de base suivantes :

- Nom du fournisseur
- Code
- Contacts (Nom et e-mail)
- Cyberscore fournisseur

Il contient également des informations plus détaillées pour chaque fournisseur, telles que :

- Date de dernière diligence cyber
- Liste des contrats et éléments du contrat

SURVEILLANCE DES INCIDENTS

Ce rapport se présente sous forme d'un tableau détaillant les incidents sélectionnés.

☛ *Pour des informations générales concernant les incidents, voir Collecte des incidents.*

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez les filtres pour trouver le rapport **Surveillance des incidents**.

Illustration

Tableau / Matrice

Paramètre du rapport

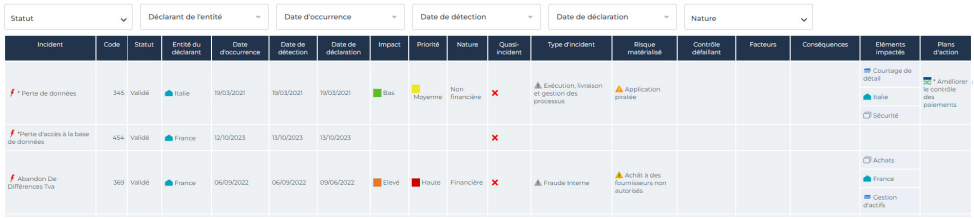
Paramètre
Liste d'incidents

Contenu du rapport

Ce rapport se présente sous forme de tableau et contient les colonnes suivantes :

- Nom
- Code
- Statut
- Entité du déclarant
- Date d'occurrence
- Date de détection
- Date de déclaration
- Impact
- Priorité
- Nature
- Quasi-incident
- Risque matérialisé
- Contrôle défaillant
- Facteurs
- Conséquences de risque
- Éléments impactés
- Plans d'action

Exemple de rapport



Statut | Déclarant de l'entité | Date d'occurrence | Date de détection | Date de déclaration | Nature

Incident	Code	Statut	Entité du déclarant	Date d'occurrence	Date de détection	Date de déclaration	Impact	Priorité	Nature	Quasi-incident	Type d'incident	Risque matérialisé	Contrôle défaillant	Facteurs	Conséquences	Eléments impactés	Plans d'action
* Perte de données	345	Validé	Italie	19/03/2021	19/03/2021	19/03/2021	Bas	Moyenne	Non financière	✕	Exécution, livraison et gestion des processus	Application pénale				Courtage de détail Italie Sécurité	* Améliorer le contrôle des paiements
*Perte d'accès à la base de données	454	Validé	France	12/10/2023	13/10/2023	13/10/2023				✕							
Abandon De Différences Tva	369	Validé	France	06/09/2022	06/09/2022	09/06/2022	Elevé	Haute	Financière	✕	Fraude interne	Achat à des fournisseurs non autorisés				Achats France Gestion d'actifs	

IMPACTS D'UN INCIDENT

Ce rapport se présente sous la forme d'un dendrogramme illustrant les impacts d'un incident.

☛ *Pour des informations générales concernant les incidents, voir Collecte des incidents.*

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Incidents.**
2. Ouvrez les propriétés d'un incident et dans la page **Reporting**, sélectionnez **Impacts d'un incident**.

Illustration

Dendrogramme

Paramètre du rapport

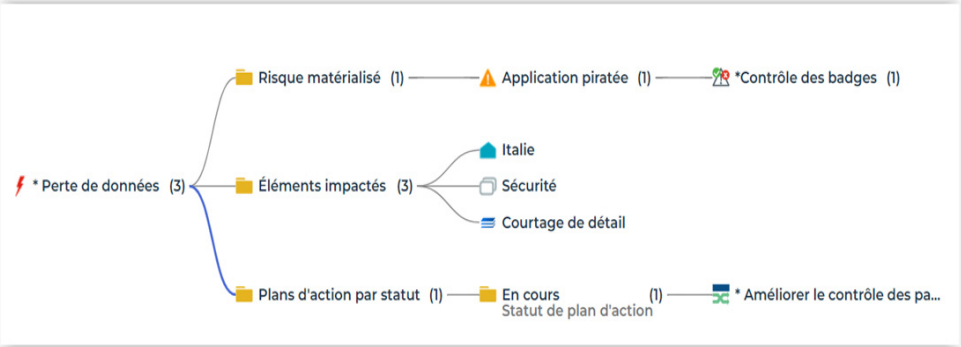
Paramètre
1 Incident

Contenu du rapport

Ce rapport indique:

- les **Plans d'action**, par statut et priorité
- l'**Analyse causale** (facteurs de risque et conséquences de risque)
- le **Risque matérialisé**, avec :
  - des informations concernant les dernières évaluations
  - les contrôles reliés au risque
  - les plans d'action par statut et priorité
- le **Contrôle défaillant**, avec :
  - des informations concernant les dernières évaluations (dernier niveau de contrôle)
  - les plans d'action par statut et priorité
- les **Éléments impactés**
  - Entité
  - Catégorie de processus
  - Processus
  - Application
  - Technologie
  - Serveur
  - Site
  - Centre de données
  - Installation
  - Ligne métier
  - Produit

Exemple de rapport

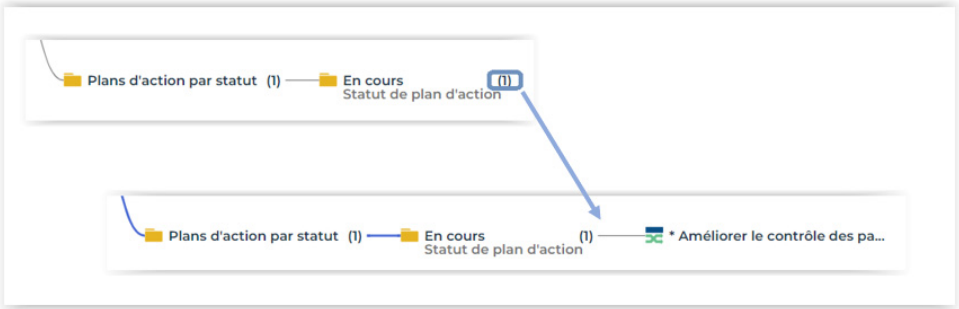


Pour visualiser des informations concernant un élément impacté :

- Passez la souris sur cet élément pour faire apparaître une info-bulle.

Pour faire apparaître des éléments d'une branche :

- Cliquez sur le chiffre qui apparaît à côté d'un élément.
  L'arborescence se déplie.



RAPPORT (MS-WORD) DES INCIDENTS MAJEURS

Un rapport MS-Word permet de déclarer les incidents aux autorités.

☛ *Pour des informations générales concernant les incidents, voir Collecte des incidents.*

Chemin d'accès

Le rapport MS-Word d'incidents majeurs peut être créé :

- à partir d'un incident
- à partir d'une liste d'incidents

Pour générer le rapport d'incidents majeurs à partir d'une liste d'incidents :

1. Dans la barre de navigation, sélectionnez **Incidents**.
2. Sélectionnez les incidents à faire figurer dans le rapport.
3. Cliquez sur ⋮ puis sélectionnez **Documentation > Rapport d'incidents majeurs**.

Illustration

Rapport MS-Word

Contenu du rapport

Le rapport d'incidents majeurs contient les éléments suivants :

Informations de base sur l'incident

- **Code - nom**
- Incident **Majeur** (Oui/Non)
- **Entité**
- **Date de détection**
- **Priorité**
- **Impact**
- Nombre de **PCA** (Plans de Continuité d'Activité)

Informations détaillées

- incident **Majeur** (Oui/Non)
- **Priorité**
- **Impact**
- **Statut**
- **Date d'occurrence**
- **Date de déclaration**
- **Date de détection**
- **Déclarant de l'incident**
- **Entité du déclarant**

Analyse des causes

- **Type d'incident** (type de risque)
- **Risque matérialisé**
- **Contrôle défaillant**

Éléments impactés

- **Entité**
- **Catégorie de processus**
- **Processus**
- **Application**
- **Technologie**
- **Serveur**
- **Site**
- **Centre de données**
- **Installation**
- **Ligne métier**
- **Produit**

Analyse financière

- **Perte brute réelle**
- **Récupérations**
- **Perte nette**
- **Perte nette réelle**

PCA déclenchés

- **Nom**
- **Statut**
- **Date de début**
- **Date de fin**
- **Résultat**

ANALYSE NŒUD PAPILLON D'UN INCIDENT

Cette analyse nœud papillon permet de visualiser graphiquement, sur un incident :

- les causes (facteurs de risque)

  📖 *Un facteur de risque est un élément qui contribue à l'apparition d'un risque ou qui en est le déclencheur. Un même facteur de risque peut être à l'origine de plusieurs risques différents. Exemples : l'utilisation d'un produit chimique dangereux, la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, etc.*

- les conséquences

  📖 *Une conséquence de risque peut être positive ou négative. Elle est associée à un type qui permet de la caractériser, par exemple : image, environnement, employés.*

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Incidents.**
2. Ouvrez les propriétés d'un incident et dans la page **Reporting**, sélectionnez **Analyse nœud papillon**.

Illustration

Analyse nœud papillon

Paramètre du rapport

Paramètre
1 Incident

Exemple de rapport

IMPACTS D'UN PROCESSUS

Ce rapport présente une vue globale d'un processus et des éléments le constituant, par exemple :

- processus
- opérations
- applications
- technologies
- risques
- contrôles
- incidents
- plans d'action
- sites
- serveurs (déployés)
- centres de données
- installations

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Processus**.
2. Dépliez la hiérarchie des catégories de processus / processus et ouvrez les propriétés d'un processus.
3. Dans la page **Reporting** du processus, sélectionnez **Rapports > Impacts du processus**.

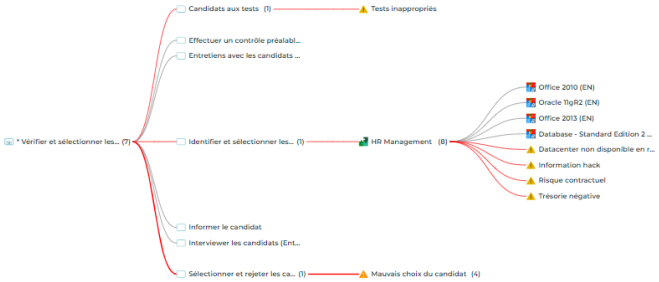
Illustration

Analyse nœud papillon

Paramètre du rapport

Paramètre
1 Processus

Exemple de rapport



Pour visualiser des informations concernant un élément impacté :

- Passez la souris sur cet élément pour faire apparaître une info-bulle.

Pour faire apparaître des éléments d'une branche :

- Cliquez sur le chiffre qui apparaît à côté d'un élément.
  L'arborescence se déplie.

  ☛ *La présence de risques dans le dendrogramme se matérialise par un lien de couleur rouge.*

VUE D'ENSEMBLE DES IMPACTS TIC DES PROCESSUS

Chemin d'accès

Menu de navigation > Rapports

Illustration

Tableau

Paramètre du rapport

Paramètre
Liste de processus

Contenu du rapport

Ce rapport présente sous forme de tableau une analyse d'impact des processus sélectionnés.

Colonnes du tableau

Colonne	Filtre	Commentaire
Processus	X	
Type de ressource TIC	X	
Ressource TIC	X	
Risque		Risque relié à la ressource TIC
Risque résiduel	X	

Colonne	Filtre	Commentaire
Plan d'action du risque		
Statut du plan d'action du risque	X	
Priorité du plan d'action du risque	X	Plan d'action relié au risque
Contrôle		
Niveau de contrôle		
Plan d'action du contrôle		
Statut du plan d'action du contrôle	X	
Priorité du plan d'action du contrôle	X	

Exemple de rapport

Processus	Type de ressource TIC	Ressource TIC	Risque	Risque résiduel	Plan d'action du risque	Statut du plan d'action du risque	Priorité du plan d'action du risque	Contrôle	Niveau de contrôle	Plan d'action du contrôle	Statut du plan d'action du contrôle	Priorité du plan d'action du contrôle
Négocier un Contrat	Application	Billing	*Paiements non effectués	Moyen	* Améliorer le contrôle des paiements	En cours	Critique	Contrôle commandes exceptionelles	Satisfaisant	* Améliorer le contrôle des paiements	En cours	Critique
								Contrôle validités des besoins	Satisfaisant	* Améliorer le contrôle des paiements	En cours	Critique
										Examen annuel des comptes	En cours	Critique
			Achat non validé financièrement	Faible								
			Facture payée 2 fois	Moyen	Examen annuel des comptes	En cours	Critique	Contrôle des paiements en double	Satisfaisant			
			Haute Indisponibilité de l'application	Elevé								
			Intrusion du système	Elevé				Contrôle Trimestriel d'accès à l'ERP				
			Inventory data modification	Elevé								

TABLEAU DE BORD DES RISQUES PAR TYPE DE RISQUE

Ce rapport se présente sous la forme d'un tableau de bord présentant les risques, contrôles et incidents reliés à un type de risque. Plusieurs types de représentation sont disponibles à l'intérieur de ce rapport.

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez éventuellement les filtres pour trouver le rapport **Tableau de bord des risques par type de risque**.

Illustrations

Ce tableau de bord se compose de divers types d'illustrations :

- Graphiques circulaires
- Cartographies
- Graphique linéaire

Paramètre du rapport

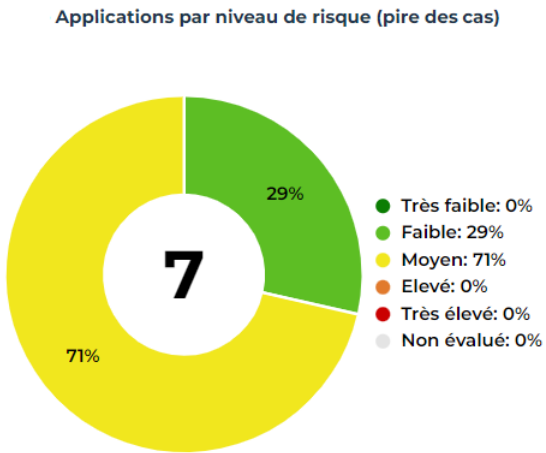
Paramètre
Type de risque

Contenu du tableau de bord

Niveaux de risque résiduel

Des graphiques circulaires affichent le niveau de risque résiduel pour plusieurs types d'objet (scénario du pire) :

- Processus
- Applications
- Technologies
- Fournisseurs
- Sites
- Serveurs (déployés)
- Installations
- Centres de données

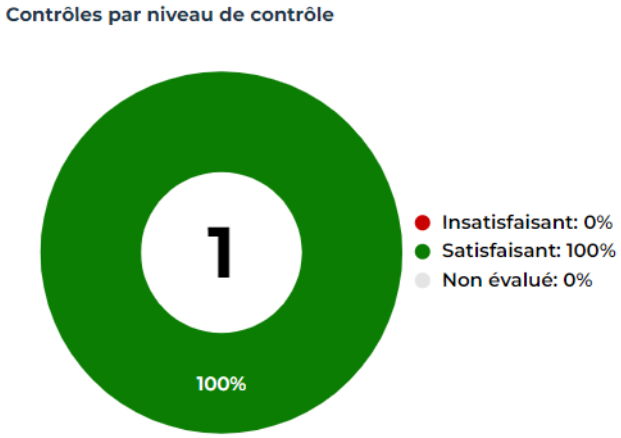


Dans l'exemple ci-dessus, 71% des processus ont un niveau de risque jugé "Moyen".

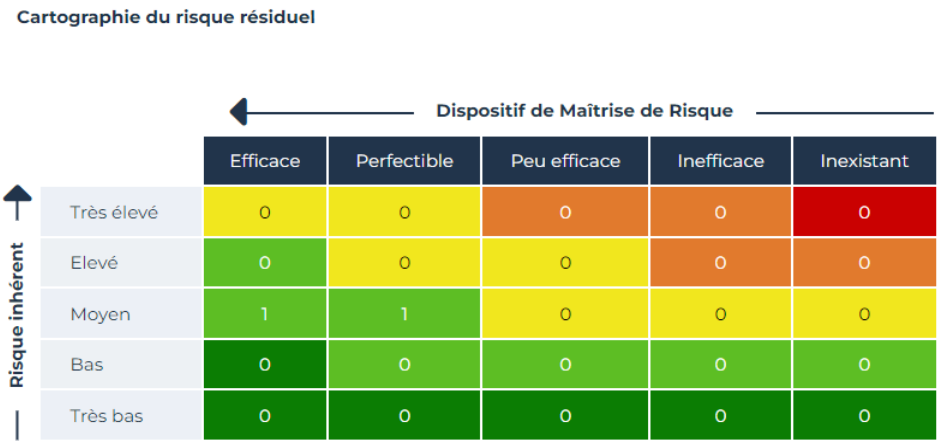
Contrôles par niveau de contrôle

Un graphique circulaire indique la répartition des contrôles par niveau de contrôle :

- Contrôles satisfaisants
- Contrôles insatisfaisants
- Contrôles non évalués

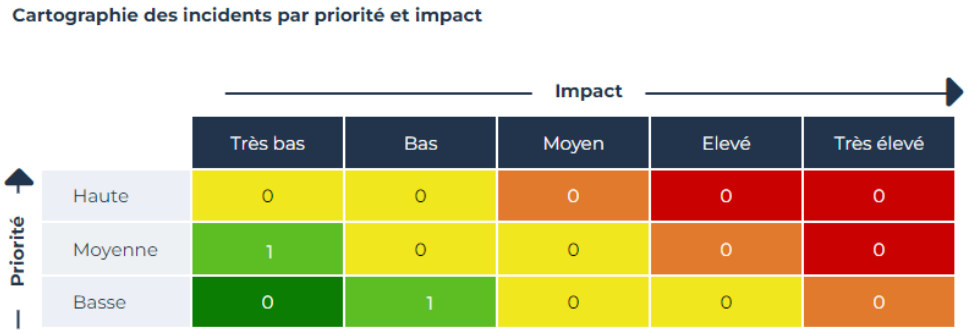


Cartographie du risque résiduel



	Efficace	Perfectible	Peu efficace	Inefficace	Inexistant
Très élevé	0	0	0	0	0
Elevé	0	0	0	0	0
Moyen	1	1	0	0	0
Bas	0	0	0	0	0
Très bas	0	0	0	0	0

Cartographie des incidents par impact et priorité



Évolution des incidents sur l'année écoulée

Un graphique linéaire affiche l'évolution des incidents sur un an. Il fait apparaître :

- horizontalement, le mois de détection de l'incident
- verticalement, le nombre d'incidents détectés durant ce mois

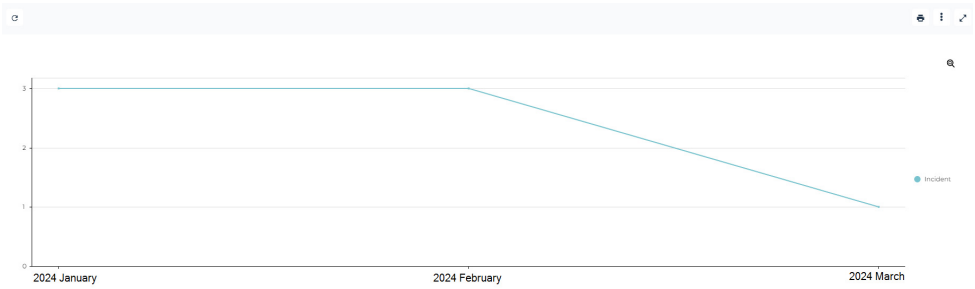


TABLEAU D'ENSEMBLE DE CRITICITÉ DES PROCESSUS ET DES ACTIFS TIC DE SUPPORT

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez éventuellement les filtres pour trouver le rapport **Tableau d'ensemble de criticité des processus et des actifs TIC de support**.

Illustrations

Tableau / Matrice

Paramètres du rapport

Paramètres	
Liste de processus	Facultatif
Entité	Obligatoire

Contenu du rapport

Ce tableau présente :

- le résultat du dernier BIA concernant les processus et l'entité sélectionnés
- l'analyse d'impact affichant la liste des actifs TIC qui supportent les processus

Les colonnes suivantes sont affichées :

- **Processus**
- **Niveau de criticité** : dernier niveau de criticité calculé sur le BIA relié au processus et à l'entité
- **Type d'actif TIC**
  - Application
  - Technologie logicielle
  - Serveur déployé
  - Site
  - Centre de données
  - Installation
  - Fournisseur
- **Actif TIC** : nom de l'actif TIC
- **Risque** : risque relié à l'actif TIC à risque
- **Risque résiduel** : dernier risque résiduel sur le risque avec l'actif TIC en contexte
- **Plans d'action du risque** : plan d'action relié au risque (statut "À démarrer" ou "En cours"
- **Contrôle** : contrôle relié au risque
- **Niveau de contrôle**
- **Plans d'action du contrôle** : plan d'action relié au contrôle (statut "À démarrer" ou "En cours")

Exemple

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						

VUE D'ENSEMBLE DES FOURNISSEURS PAR PROCESSUS

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez éventuellement les filtres pour trouver le rapport **Vue d'ensemble des fournisseurs par processus**.

Illustrations

Tableau / Matrice

Paramètres du rapport

Paramètres	
Processus critiques	Obligatoire

☛ *Un processus est dit "critique" lorsque le résultat d'un BIA est considéré "critique" d'après la définition du modèle de BIA. Pour plus de détails, voir Gérer les valeurs d'impact sur l'activité.*

Contenu du rapport

Ce tableau présente une vue globale des fournisseurs impliqués dans les processus sélectionnés.

Les colonnes suivantes sont affichées :

- **Processus critique**
- **Entité** : Entité du BIA
- **Date de BIA** : Date de fermeture du BIA
- **Impact sur l'activité**
- **Contrat** : contrat en vigueur
- **Type de contrat**
- **Code**
- **Fournisseur** : fournisseur impliqué dans le processus (avec contrat en vigueur)
- **Cyberscore**
- **Ressource**
- **Date de début du contrat**
- **Date de fin du contrat**
- **Pièces jointes** (en nombre, avec un lien vers la liste des pièces jointes)

Exemple

Processus critique	Entité	Date de BIA	Impact sur l'activité	Contrat	Type de contrat	Code	Fournisseur	Cyberscore	Actif	Date de début de contrat	Date de fin de contrat	Pièces jointes
* Rechercher, sélectionner et recruter des collaborateurs	France	19/09/2023	Moyen	Contrat-3			Adobe Systems (EN)		* Rechercher, sélectionner et recruter des collaborateurs	01/10/2024	24/10/2024	0
Développer et gérer le planning, la réglementation et la stratégie RH	France	19/09/2023	Moyen									
Gérer les Compétences et la Formation des Collaborateurs	France	20/09/2023	Faible									
Gérer les informations des salariés	France	20/09/2023	Critique	Contrat-1			Microsoft Azure		* Apache log4j v2.17 (EN) * MEGA BANK Mobile App (EN) Gérer les informations des salariés	15/10/2024	31/10/2024	0

ACTIFS TIC CRITIQUES (À PARTIR DE PROCESSUS/ENTITÉ)

Chemin d'accès

Pour accéder à ce rapport :

1. Dans la barre de navigation, sélectionnez **Rapports > Créer un rapport.**
2. Utilisez éventuellement les filtres pour trouver le rapport **Actifs TIC critiques (à partir de Processus ou Entité)**.

Illustration

Tableau / Matrice

Paramètres du rapport

Paramètres	
Processus ou Entité	Obligatoire
Type de risque	Facultatif

Contenu du rapport

Ce rapport se présente sous forme de tableau et contient les colonnes suivantes :

- **Processus critique**

  ☛ *Un processus est dit "critique" lorsque le résultat d'un BIA est considéré "critique" d'après la définition du modèle de BIA. Pour plus de détails, voir Gérer les valeurs d'impact sur l'activité.*

- **Entités**
- **Type d'actif TIC**
- **Actif TIC**
- **Risque**
- **Impact**
- **Probabilité**
- **Risque inhérent**
- **Dispositif de Maîtrise de Risque**
- **Risque résiduel**
- **Plan d'action du risque**
- **Contrôle**
- **Niveau de contrôle**
- **Plan d'action du contrôle**

Exemple de rapport

Processus critique	Entités	Type d'actif TIC	Actif TIC	Risques	Impact	Probabilité	Dispositif de Maîtrise de Risque	Risque inhérent	Risque résiduel	Plans d'action du risque	Statut de plan d'action du risque	Priorité de plan d'action du risque	Contrôles	Niveau de contrôle	Plans d'action du contrôle	Priorité de plan d'action du contrôle	Statut de plan d'action du contrôle
* Rechercher, sélectionner et recruter des collaborateurs	• France	Application	CRM Europe	Haute Indisponibilité de l'application													
				Marché du travail tendu	Très élevé	Probable	Peu efficace	Très élevé	Elevé								
				Risque de vol de données													
				Technologie obsolète	Bas	Possible	Inefficace	Bas	Faible								
		Technologie logicielle	Office 2013 (EN)	Obsolescence	Très bas	Probable	Inefficace	Bas	Faible								
			SAP NetWeaver (EN)														
			SQL Server - Enterprise - 14.0 (EN)														