HOPEX Risk Mapper

Guide d’utilisation

HOPEX V2

INTRODUCTION

Gérer les risques, assurer et maintenir la conformité aux nouvelles réglementations représentent une vraie opportunité pour qui veut piloter les transformations de l'entreprise. Dans cette perspective, **HOPEX Risk Mapper** offre une visibilité complète sur les risques auxquels fait face l'entreprise, en particulier les risques opérationnels, les points de contrôle et les chaînes de valeur.

Le référentiel **HOPEX** couvre toutes les ressources de l'entreprise, des chaînes de valeur globales aux ressources informatiques. L'approche de **HOPEX Risk Mapper** permet aux responsables métiers et informatiques de garantir la traçabilité des contrôles de conformité au travers des couches applicatives, des données et des infrastructures.

Avec **HOPEX Risk Mapper**, il est plus facile d'intégrer la politique de gestion des risques et les contrôles de conformité à la gouvernance d'entreprise : en fixant des objectifs réalistes d'une part, et en fournissant d'autre part des livrables et des informations indispensables à tous les acteurs impliqués.

- ✓ "Le processus de gestion des risques", page 2
- ✓ "Se connecter à HOPEX Risk Mapper", page 5
- ✓ "Présentation de l'interface", page 7
- ✓ "A propos de ce guide", page 11

LE PROCESSUS DE GESTION DES RISQUES

Associé à l'ensemble des produits de la suite **HOPEX**, **HOPEX Risk Mapper** permet de modéliser l'environnement, d'évaluer les risques puis de les traiter et enfin, de les maîtriser grâce à une politique de contrôle efficace.

Le processus recommandé par **HOPEX** est donc composé des étapes suivantes :

- *"Modéliser l'environnement", page 2*,
- *"Identifier, analyser et évaluer les risques", page 2*,
- *"Traiter les risques", page 3*,
- *"Suivi opérationnel et politique de contrôle", page 3*.

Modéliser l'environnement

Le contexte dans lequel les risques doivent être gérés comprend l'environnement externe et interne de l'organisation, ses objectifs stratégiques, ainsi que les objectifs spécifiques de l'activité de gestion des risques.

- Environnement externe définit l'environnement externe dans lequel l'organisation opère, ainsi que ses relations avec cet environnement.

  ☛ *Pour plus de détails, voir "Environnement externe", page 19.*

- Environnement interne décrit l'organisation. Cela permet à la gestion des risques de tenir compte des principaux objectifs et des principales contraintes de l'organisation.

  ☛ *Pour plus de détails, voir "Environnement interne", page 14.*

- Le contexte de la gestion des risques est essentiellement lié aux objectifs que l'entreprise poursuit à travers son projet de gestion des risques.

  ☛ *Pour plus de détails, voir "Contexte de la gestion des risques", page 26.*

Identifier, analyser et évaluer les risques

Il est nécessaire d'identifier les risques concernés, puis de les analyser et enfin d'en faire une estimation afin de disposer des éléments nécessaires à leur traitement éventuel.

Identifier les risques

Il est nécessaire de déterminer où, quand, pourquoi et comment des événements peuvent empêcher, dégrader ou améliorer l'atteinte des objectifs de l'organisation.

Les événements internes et externes susceptibles d'affecter l'atteinte de ces objectifs doivent être décrits en faisant la distinction entre risques et opportunités. Les opportunités peuvent ensuite être prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs.

Plus particulièrement, il est possible de proposer plusieurs méthodes d'identification des risques en fonction du contexte.

- Méthode basée sur l'atteinte des objectifs de l'organisation ;
- Méthode basée sur des listes de types de risques, de facteurs de risques ou de types de contrôles appliquées à un contexte d'apparition ;
- Méthode basée sur des données historisées (bases d'incidents, de réclamations ou de défauts).

☛ *Pour plus de détails, voir "Identifier les risques", page 34.*

Analyser les risques

Il s'agit de compléter l'identification de chaque risque en indiquant précisément ce qui peut arriver, où, quand, pourquoi et comment cela peut arriver. Cette analyse peut amener à la découverte de nouveaux risques qui n'avaient pas été identifiés directement lors de l'étape précédente. On évalue également l'efficacité des contrôles existants qui peuvent permettre de prévenir ce risque.

☛ *Pour plus de détails, voir "Analyse des risques", page 41.*

Evaluer les risques

Après avoir identifié et analysé les risques encourus par l'entreprise, l'étape suivante consiste à estimer leur importance de manière à mettre en évidence les risques les plus importants à traiter.

Les risques sont estimés en prenant en compte :

- leur fréquence d'occurrence
- leur impact.

☛ *Pour plus de détails, voir "Evaluer les risques", page 44.*

Traiter les risques

L'évaluation des risques constitue ainsi une étape essentielle pour obtenir une liste des risques pouvant nécessiter un traitement, avec un ordre de priorité.

En s'appuyant sur les évaluations réalisées précédemment, le niveau acceptable pour chaque risque est défini.

☛ *Pour plus de détails, voir "Le traitement du risque", page 50.*

Traiter les risques implique :

- l'identification des différentes options possibles,
- l'évaluation de ces options
- la préparation et la mise en œuvre des plans de traitement :
  - *"Mise en place des plans d'action", page 53*
  - *"Les contrôles", page 54*

Suivi opérationnel et politique de contrôle

Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et l'application effective des mesures de traitement des risques.

Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

Les axes présentés dans ce guide sont les suivants :

- "Amélioration continue des dispositifs de contrôle", page 62.
- "Evaluation de l'efficacité des contrôles", page 63.
- "Suivi des incidents et des pertes", page 64.

Information et communication

Les informations utiles sont identifiées, collectées, et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace.

L'information et la communication sont fondamentales à chaque étape du processus de gestion des risques. Elles doivent impliquer un dialogue avec les différentes parties prenantes avec un effort particulier sur les remontées du terrain plutôt qu'un flux d'information à sens unique depuis les décideurs vers les opérationnels.

☛ *Pour plus de détails sur les fonctionnalités offertes par **HOPEX**, voir le guide **HOPEX Common Features**, qui décrit les outils spécifiques aux solutions **HOPEX**.*

SE CONNECTER À HOPEX RISK MAPPER

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

Se connecter à la solution

Pour se connecter à **HOPEX Risk Mapper**, voir HOPEX Common Features, "Le bureau HOPEX Web Front-End".

Gérer les options relatives aux risques

Les fonctionnalités décrites dans ce guide s'appuient sur de nouvelles facilités de gestion des risques mises en oeuvre dans la version **HOPEX V2** de **HOPEX**.

Toutefois, des options de comptabilité sont proposées afin de transférer vos données d'une version à l'autre ou de continuer à travailler avec les fonctionnalités proposées par **HOPEX Control and Risk**, par exemple.

Pour pouvoir accéder aux fonctionnalités de gestion des risques proposées dans les versions de **HOPEX** antérieures à la version **HOPEX V2** :

1. Ouvrez la fenêtre des options.
2. Dans la partie gauche de la fenêtre, cliquez sur le dossier **Compatibilité** puis sur le dossier **Autres**.
3. Dans la partie droite, cochez l'option **Compatibilité propriétés des risques (MEGA 2009)**.

Cette option vous permet, par exemple, de voir apparaître dans la fenêtre de propriétés des risques des onglets tels que **Analyse**, **Situation** ou **Redondance**.

Par défaut, seules les facilités de gestion des risques mises en oeuvre dans la version **HOPEX V2** de **HOPEX** sont proposées. Vous pouvez continuer à utiliser les facilités et la présentation des versions de **HOPEX** antérieures à cette version.

Pour activer l'option de compatibilité :

1. Dans l'espace de travail, ouvrez la fenêtre des **Options**.
2. Faites un double-clic sur l'icône **Modélisation des processus et de l'architecture**.
3. Cochez l'option **Compatibilité propriétés des risques HOPEX**.

☺ *Un article technique de migration " CRK to ERM ICM Risk Mapper Data Migration Toolkit " est disponible sur la communauté dans la section " technical articles ". Cet article détaille le fonctionnement des outils de migration des données de **MEGA Control and Risk** au format **HOPEX Risk Mapper / HOPEX Enterprise Risk Management** proposés en standard (cf. outil de conversion).*

Les profils de HOPEX Risk Mapper

Dans **HOPEX Risk Mapper** il existe, par défaut, des profils auxquels sont associés des droits et accès.

La présentation de l'interface de la solution dépend du profil sélectionné par l'utilisateur lors de sa connexion à l'application ; l'arborescence des menus et les fonctionnalités sont différentes d'un profil à l'autre.

Les profils disponibles sont :

- Architecte Contrôles et Risques ;
- Risk Manager (simplifié).

Profils	Tâches
Architecte Contrôle et Risques	L'architecte Contrôle et Risques travaille avec les outils de modélisation proposés par **HOPEX**. Il est responsable de l'identification et de l'évaluation des risques sur le périmètre dont il a la charge. - Identification des risques - Évaluation directe - Création des rapports d'analyse.
Risk Manager (simplifié)	Le Risk Manager (simplifié) dispose d'une solution proposée par **HOPEX Solutions**. Comme l'architecte Contrôle et Risques, il est responsable de l'identification et de l'évaluation des risques sur le périmètre dont il a la charge, mais il ne dispose pas de l'ensemble des facilités de modélisation de **HOPEX**. Par exemple, il ne peut pas utiliser les diagrammes.

PRÉSENTATION DE L'INTERFACE

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

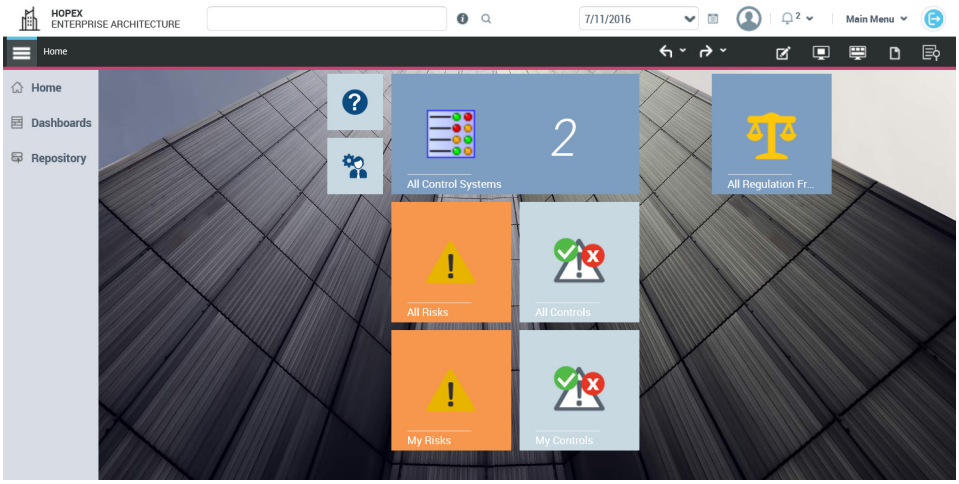
☛ *Pour plus de détails sur l'utilisation générale de l'interface, voir le guide **HOPEX Common Features**.*

☛

Présentation de l'architecte Contrôle et Risques

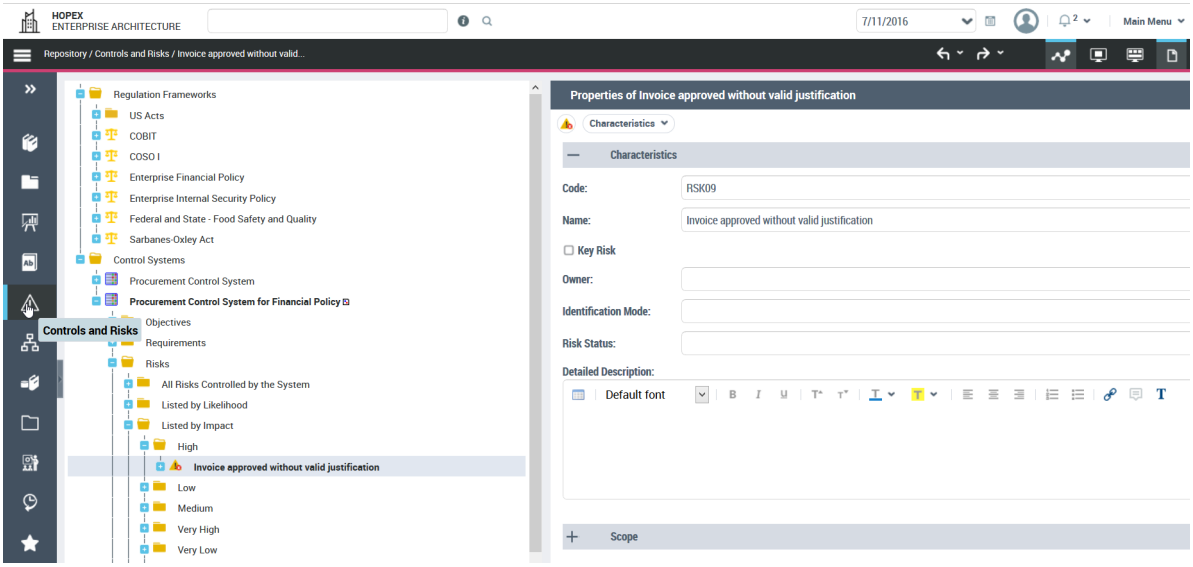
L'architecte Contrôle & Risques dispose d'un bureau de modélisation qui présente les objets dont il a la charge.

☛ *Pour plus de détails, voir "Les profils de HOPEX Risk Mapper", page 6.*



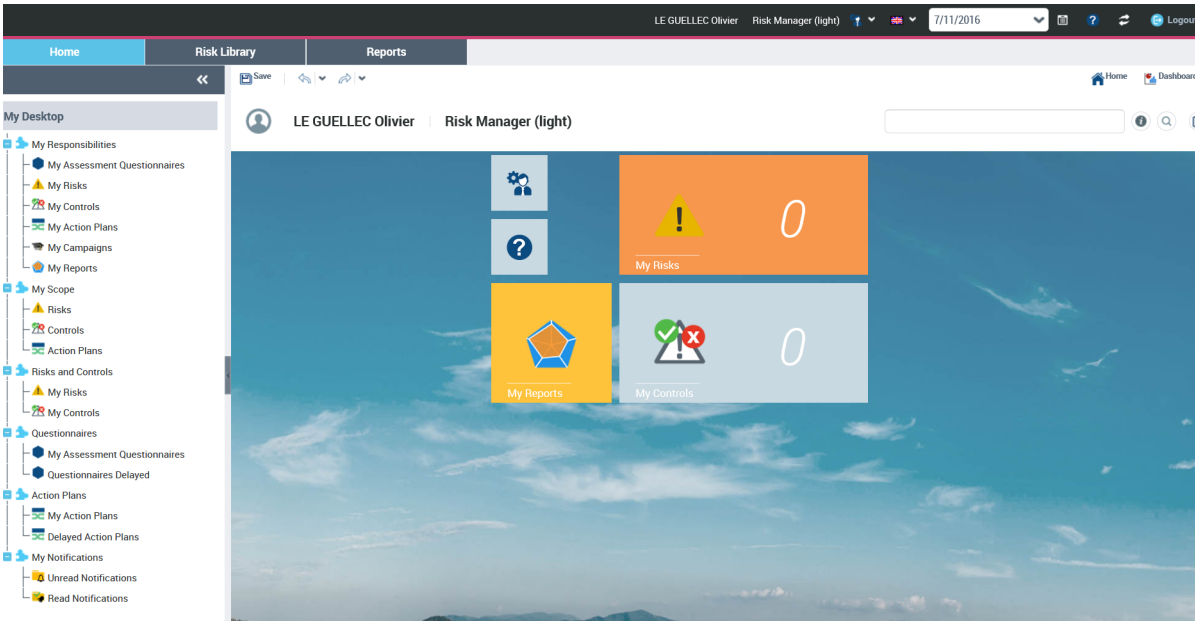
Le bureau de l'architecte Contrôle & Risques présente les volets suivants :

- **Accueil** : permet d'accéder facilement aux différents dossiers et objets dont l'utilisateur a la responsabilité à travers des tuiles :
  - **Tous les dispositifs**,
  - **Tous les cadres réglementaires**,
  - **Tous les risques** et **mes risques**,
  - **Tous les contrôles** et **mes contrôles**.
- **Référentiel** : permet d'accéder à la liste des risques et des contrôles.



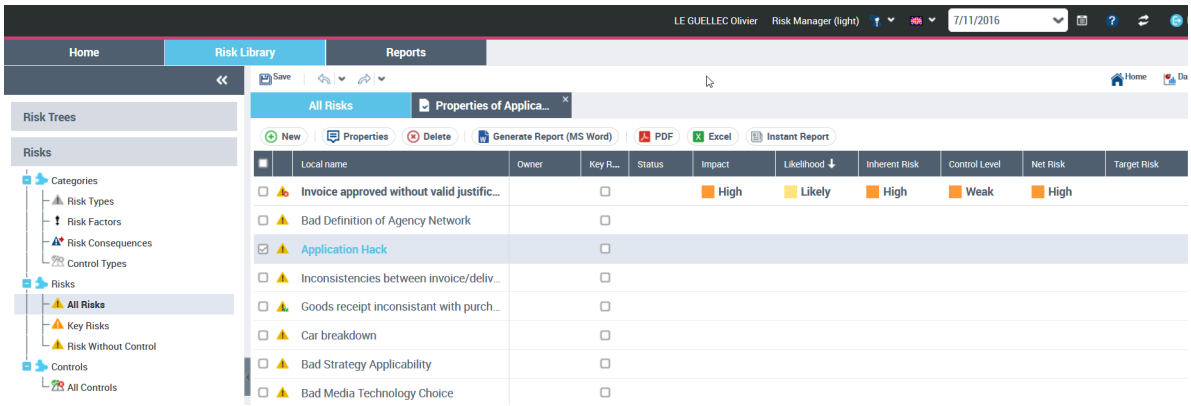
Bureau du Risk Manager (simplifié)

☛ *Pour plus de détails sur le rôle du Risk Manager (simplifié), voir "Les profils de HOPEX Risk Mapper", page 6.*



Le Risk Manager (simplifié) dispose d'un bureau de gestion des risques qui présente les onglets suivants :

- **Accueil** : permet d'accéder facilement aux différents dossiers et objets dont l'utilisateur a la responsabilité à travers des tuiles :
  - **Mes risques**,
  - **Mes contrôles**,
  - **Mes rapports**.
- **Référentiel** : permet d'accéder à la liste des risques et des contrôles. Il est possible de faire des évaluations directes à partir de cet onglet.
- **Rapports** : donne accès à l'ensemble des rapports permettant l'analyse et le suivi de la mise en œuvre des contrôles et des risques.



A PROPOS DE CE GUIDE

Ce guide vous présente comment tirer parti de **HOPEX Risk Mapper** pour assurer une gestion efficace de vos risques.

Structure du guide

La structure du guide **HOPEX Risk Mapper** est liée à la méthodologie recommandée par **HOPEX**. Il est donc composé des chapitres suivants :

- "Analyse de l'environnement", page 13, présente comment décrire, avec **HOPEX Risk Mapper,** l'environnement interne et externe de votre organisation ainsi que le contexte dans lequel s'inscrit votre projet de gestion des risques ;
- "Évaluer les risques", page 33, présente les fonctionnalités proposées par **HOPEX Risk Mapper** pour déclarer et analyser les incidents ;
- "Le traitement des risques et les contrôles", page 49, présente les fonctionnalités proposées par **HOPEX Risk Mapper** pour déclarer et analyser les incidents ;
- "Suivi opérationnel de la politique de contrôle", page 61, présente les possibilités d'utilisation et de maintenance de objets mis en place dans le cadre de la politique de gestion des risques ;
- "Les rapports HOPEX Risk Mapper", page 65, présente les rapports proposés par **HOPEX Risk Mapper** pour analyser les risques ;

Ressources complémentaires

Ce guide est complété par :

- le guide **HOPEX Common Features**, qui décrit l'interface Web et les outils spécifiques aux solutions HOPEX,

  ☛ *Il peut être utile de consulter ce guide pour une présentation générale de l'interface.*
- le guide du produit **HOPEX Business Process Analysis**, qui décrit les fonctionnalités proposées pour la modélisation des processus et applications de votre entreprise,
- le guide du produit **HOPEX Enterprise Risk Management**, qui décrit les fonctionnalités proposées pour la gestion des risques,
- le guide du produit **HOPEX LDC**, qui décrit les fonctionnalités proposées pour la gestion des incidents et des pertes,
- le guide **HOPEX Collaboration Manager**, pour plus de détails sur les plans d'action,
- le guide d'administration **HOPEX Power Supervisor**, **HOPEX Power Supervisor**, pour les gestions des profils et des rôles de vos utilisateurs.

Conventions utilisées dans le guide

Styles et mises en forme

☛ *Remarque sur les points qui précèdent.*

📖 *Définition des termes employés.*

☺ *Astuce qui peut faciliter la vie de l'utilisateur.*

Compatibilité avec les versions précédentes.

Ce qu'il faut éviter de faire.

Remarque très importante à prendre en compte pour ne pas commettre d'erreurs durant une manipulation.

Les commandes sont présentées ainsi : **Fichier > Ouvrir**.

Les noms de produits et de modules techniques sont présentés ainsi : **HOPEX**.

ANALYSE DE L'ENVIRONNEMENT

Analyser l'environnement dans lequel le projet de gestion des risques va être mené permet de définir les paramètres de base selon lesquels les risques doivent être gérés et de délimiter le périmètre du projet. Cette analyse comprend l'environnement interne et externe de l'organisation, ses objectifs stratégiques, ainsi que les objectifs spécifiques de l'activité de gestion des risques.

Ce chapitre vous présente comment décrire l'environnement d'un projet de gestion de risques avec **HOPEX Risk Mapper**.

Ce chapitre présente comment décrire et analyser, avec **HOPEX Risk Mapper**, les éléments suivants :

ENVIRONNEMENT INTERNE

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont l'ensemble des collaborateurs appréhende et prend en compte les risques, et plus particulièrement la conception du management et son appétence pour le risque, l'intégrité et les valeurs éthiques, ainsi que l'environnement dans lequel l'organisation opère.

Il est possible de recenser, à cette étape :

- la liste des *objectifs* stratégiques de l'organisation et les *exigences* associées
  Ces objectifs doivent être définis pour que le management puisse identifier les événements potentiels susceptibles d'en affecter la réalisation. La gestion des risques permet de s'assurer que les objectifs sont en ligne avec la mission de l'organisation ainsi qu'avec son appétence pour le risque.
- un état des lieux de l'existant de l'entreprise (organigramme, *processus*, *règles de gestion*, *dispositifs de contrôle*, responsabilités, *applications*, *infrastructures*)

Définir l'environnement interne permet d'assurer que la gestion des risques tient compte des principaux objectifs et des principales contraintes de l'organisation.

Acteurs internes de l'organisation

Les différents acteurs concernés doivent être impliqués à chaque étape du projet de gestion des risques à travers un processus de communication et de consultation.

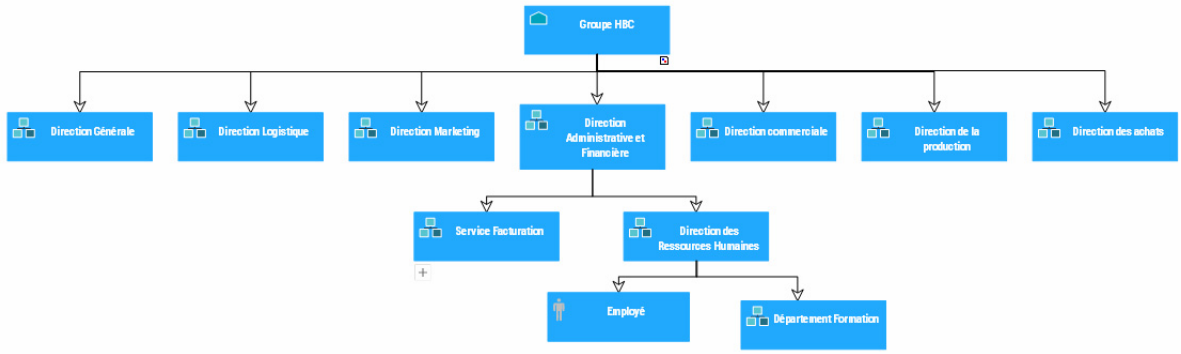
Ceci permet de construire une solution qui sera mieux acceptée par les différentes parties prenantes.

Pour accéder à l'ensemble des entités de l'organisation avec le profil ***Architecte Contrôle et Risques*** :

- A partir du volet **Référentiel**, sélectionnez **Objets principaux**, puis dépliez le dossier **Acteurs**.
  La liste des acteurs s'affiche.

Pour définir la liste des *acteurs* concernés, **HOPEX Risk Mapper** vous permet de saisir l'organigramme de l'entreprise.

Pour cela, à partir d'un acteur, sélectionnez **Nouveau > Organigramme d'acteurs**.



Organigramme hiérachique et fonctionnel de l'entreprise

> ☛ *Pour plus d'information sur les organigrammes, voir le chapitre "Organigramme et responsabilités" du guide* ***HOPEX Business Process Analysis***.
>
> ☛ *Pour accéder à l'ensemble des entités de l'organisation avec le profil* ***Risk Manager (simplifié)*** *: dans l'onglet* ***Bibliothèque des risques****, sélectionnez* ***Arborescence des risques*** *et dépliez le dossier* ***Risques par entité.***

Vous pouvez également définir des objectifs et des exigences pour chaque acteur.

Objectifs et exigences de l'organisation

Certains documents clés, tels que les plans stratégiques, le business plan, les rapports annuels, des analyses économiques et d'autres documentations pertinentes au sujet de l'organisation et de ses buts peuvent être consultés pour définir ses *objectifs* et *exigences*.

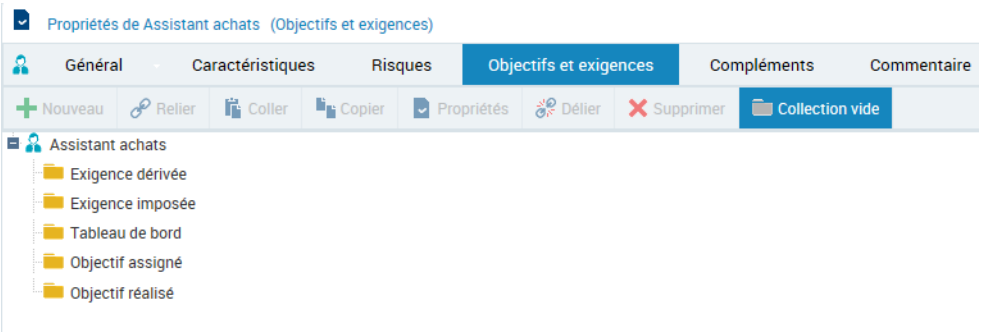
> 🕮 *Un objectif est un but que l'on cherche à atteindre ou la cible visée pour un processus ou une opération. Il permet de mettre en évidence les points que l'on veut améliorer pour ce processus ou cette opération.*
>
> 🕮 *Une exigence est un besoin ou une attente formulés explicitement, imposés comme une contrainte à respecter dans le cadre d'un projet de certification, d'organisation ou de modification du système d'information d'une entreprise.*

Avec **HOPEX Risk Mapper**, les objectifs et exigences de votre organisation sont définis dans les propriétés de l'acteur qui représente l'organisation.

Pour définir les *objectifs* et *exigences* de chaque acteur :

1. Ouvrez sa fenêtre de propriétés de l'acteur,

2. Sélectionnez l'onglet **Objectifs et exigences**.



Vous pouvez créer de nouveaux objectifs et exigences ou relier ceux qui existent déjà.

☛ *Pour plus d'information sur la définition des objectifs et les exigences, voir le chapitre "Objectifs et exigences" du guide* ***HOPEX Common Features****.*

Processus de l'organisation

Pour accéder à l'arbre des processus métier avec le profil ***Architecte Contrôle et Risques*** :

❱ A partir du volet **Référentiel**, sélectionnez **Objets principaux** puis dépliez le dossier **Processus métier**.
Si vous dépliez le dossier d'un processus, vous pouvez faire apparaître l'arbre des sous-processus détenus par le processus courant.

☛ *Pour accéder à l'ensemble des processus du référentiel avec le profil* ***Risk Manager (simplifié)*** *: dans l'onglet* ***Bibliothèque des risques****, sélectionnez* ***Arborescence des risques > Risques par processus.***

Les types de processus

Les types de processus disponibles sont :

- processus métier

🕮 *Un processus métier représente un système qui fournit des produits ou des services à un client interne ou externe à l'entreprise ou à l'organisation. Aux niveaux supérieurs, un processus métier définit une structuration et une catégorisation du métier de l'entreprise. Il peut être décomposé en d'autres processus. Le lien vers les processus organisationnels permet de décrire l'implémentation réelle du processus métier dans l'organisation. Un processus métier peut également être*

détaillé à l'aide d'une vue fonctionnelle.

- processus organisationnels

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

- processus fonctionnels

  📖 *Un processus fonctionnel est une chaîne de valeur produisant des résultats qui peuvent être des biens ou des services à un client interne ou externe à l'entreprise ou à l'organisation. Cette chaîne de valeur est décrite par une séquence d'activités.*

Les types se distinguent par une icône différente dans les arbres ou les listes.

Les onglets de la fenêtre de propriétés d'un processus

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

- **Caractéristiques** : pour présenter les différentes personnes responsables du processus. Pour plus de détails, voir "Le RACI sur un risque", page 39.
- **Risques** : liste des risques qui portent sur le processus. Pour plus de détails, voir "Évaluer les risques", page 33.
- **Objectifs et exigences** : pour plus de détails, voir "Objectifs et exigences de l'organisation", page 15.
- **Commentaires** : pour une description textuelle du processus.

Applications

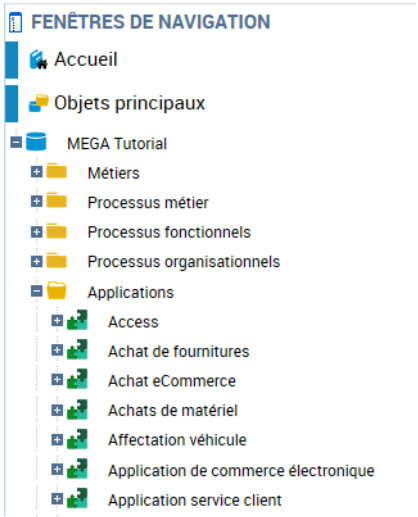
La description du contexte interne dans le cadre duquel se déroule le projet de gestion des risques peut être également complétée par la description des *applications* informatiques concernées.

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

Pour accéder aux applications avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Objets principaux**.

2. Dépliez le dossier **Applications**.
   La liste des applications définies dans la base apparaît.



Vous pouvez associer des *objectifs* et des *exigences* à chaque application.

☛ *Si vous disposez du produit **HOPEX IT Architecture**, vous pouvez également décrire le fonctionnement de l'application en tant qu'enchaînement de sous-applications ou de services. Pour plus de détails sur la description des applications, voir le guide **HOPEX IT Architecture**.*

ENVIRONNEMENT EXTERNE

Il s'agit de définir l'environnement externe dans lequel l'organisation opère, ainsi que ses relations avec cet environnement. Ceci peut inclure, par exemple :

- son environnement social, réglementaire, culturel, concurrentiel, financier et politique,
- la liste des réglementations qui impactent l'organisation et les exigences associées,
- les forces, faiblesses, opportunités et menaces auxquelles l'organisation fait face,
- la liste des parties prenantes externes à l'organisation, ainsi que leurs exigences,
- les indicateurs de performance clés.

Etablir le contexte externe permet de s'assurer que les différents acteurs externes, ainsi que leurs objectifs et exigences, sont pris en compte dans la politique de gestion des risques.

Pour décrire l'environnement externe dans lequel l'organisation opère, **HOPEX Risk Mapper** vous permet de définir :

- la liste des réglementations qui impactent l'organisation et les exigences associées, voir "Les cadres réglementaires", page 19,
- la liste des parties prenantes externes à l'organisation, ainsi que leurs objectifs et exigences, voir "Les acteurs externes : objectifs et exigences", page 24.

Les cadres réglementaires

> 🕮 *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.*

Accéder aux cadres réglementaires de l'organisation

Pour accéder à la liste des cadres réglementaires avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et Risques**, puis dépliez le dossier qui correspond à votre référentiel.
   Les deux dossiers **Cadres réglementaires** et **Dispositifs de contrôle** apparaissent.
2. Dépliez le dossier **Cadres réglementaires**.
   La liste des cadres réglementaires de l'organisation s'affiche.

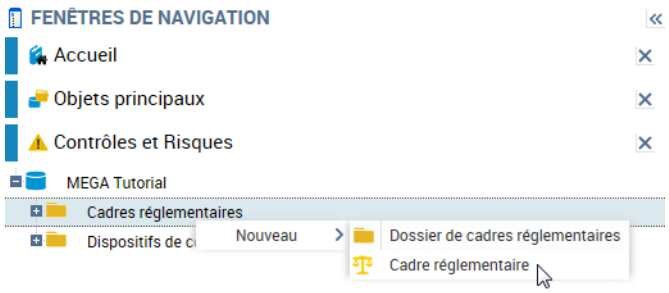
> ☺ *Vous pouvez importer dans votre référentiel des bibliothèques contenant la description d'un cadre réglementaire avec les exigences, type de risques, facteurs de risques ou types de contrôles qui y sont associés.*
>
> ☛ *Il peut également y avoir des cadres réglementaires internes à l'organisation pouvant servir de guide de gouvernance. Dans cette*

documentation, les termes "Réglementation" ou "cadre réglementaire" sont utilisés, qu'il s'agisse d'une réglementation d'origine externe ou d'un règlement interne.

Créer un cadre réglementaire

Pour créer un cadre réglementaire avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et risques**.
2. Dans le menu contextuel du dossier "Cadres réglementaires", sélectionnez **Nouveau > Cadre réglementaire**.



Une fenêtre vous demande de saisir le nom du nouveau cadre réglementaire.

3. Après avoir saisi le nom, cliquez sur **OK**.
   Le nouveau cadre réglementaire apparaît dans l'arborescence du navigateur.

Caractéristiques d'un cadre réglementaire

Pour accéder aux caractéristiques générales d'un cadre réglementaire :

1. Ouvrez la fenêtre de propriétés du cadre réglementaire.
2. Cliquez sur l'onglet **Caractéristiques**.
   Les caractéristiques présentées sont les suivantes :
   - Le **Code de la réglementation,** qui est interne,
   - La **Portée de la réglementation**, qui peut être internationale, locale à un pays ou à un groupe de pays, etc.
   - La **Date de la réglementation**, texte libre qui permet de préciser l'année ou la période d'application de la réglementation,
   - La **Date de début d'application** de la réglementation,
   - La **Date de fin d'application** de la réglementation,
   - La **Statut de la réglementation**,

     ☛ *le **Statut de la réglementation** n'est pas modifiable parce qu'il est géré par le workflow associé au cadre réglementaire. Pour plus de détails, voir le guide **HOPEX Internal Control**.*
   - La date de la **Dernière mise à jour** de la réglementation.

Classifications d'un cadre réglementaire

Pour accéder aux classifications d'un cadre réglementaire :

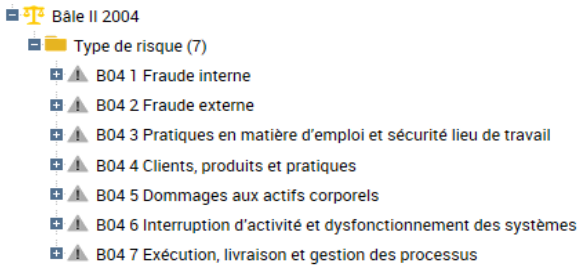
1. Ouvrez la fenêtre de propriétés du cadre réglementaire qui vous intéresse et cliquez sur le bouton **Classification**.

2. Vous pouvez sélectionnez une classification parmi les suivantes :
   - Types de risque, voir "Les types de risque", page 22 ;

     Un type de risque définit une typologie de risque normalisée dans le cadre d'une organisation.
   - Facteurs de risque, voir "Les facteurs de risque", page 23 ;

     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.
   - Types de contrôle, voir "Les types de contrôle", page 23 ;

     Un type de contrôle permet de classifier les contrôles mis en oeuvre dans l'entreprise conformément à des standards sectoriels ou réglementaires (Cobit, etc.).
3. Si vous sélectionnez **Types de risque**, par exemple, la liste des types de risques associés au cadre réglementaire s'affichent.



Exigences d'un cadre réglementaire

Pour accéder aux exigences d'un cadre réglementaire :

- Ouvrez la fenêtre de propriétés du cadre réglementaire qui vous intéresse et cliquez sur le bouton **Exigences**.

  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.

Dispositifs de contrôle d'un cadre réglementaire

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 relatif à loi Informatique & Liberté, le dispositif de contrôle de gestion, le dispositif d'audit interne.

Pour plus de détails sur les dispositifs de contrôle, voir "Les dispositifs de contrôle", page 27.

Les types de risque

C'est en regroupant des événements potentiels similaires que le management peut améliorer son processus d'identification des opportunités et des risques.

Les entreprises peuvent classer les événements potentiels pour s'assurer que les efforts déployés en terme d'identification sont exhaustifs. Cette classification peut également contribuer à développer par la suite une vision globale des risques.

> 🕮 *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.

La décomposition des types de risque sera propre aux différentes activités et selon la ligne de métier ou l'activité particulière. Il pourra y avoir une plus ou moins grande décomposition des types de risques génériques en niveaux de types de risques spécifiques.

Il est important de se doter d'un cadre de définition d'un type de risque identifiable, mesurable, gérable et de se limiter dans le nombre de niveaux pour conserver une nomenclature exploitable.

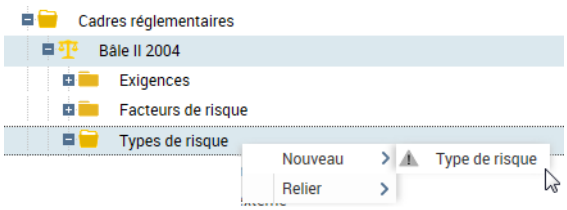
La validation de la nomenclature doit permettre de s'assurer qu'un même type de risque défini dans deux entités ou deux activités différentes aura la même définition et le même sens afin de conserver un dispositif cohérent.

Le dispositif mis en place devant répondre également à des besoins réglementaires, il sera nécessaire de définir une deuxième nomenclature afin de pouvoir répondre aux aspects déclaratifs et de pouvoir échanger avec les instances de contrôle.

> Par exemple, dans le secteur bancaire, des types de risques ont été définis dans le cadre des recommandations de Bâle II. Pour plus de détails, voir http://www.bis.org/bcbs/.
> **HOPEX** permet de prendre en compte ces types de risques.

Pour créer vos propres types de risque avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et Risques**, puis dépliez le dossier qui correspond à votre référentiel.
   Les deux dossiers **Cadres réglementaires** et **Dispositifs de contrôle** apparaissent.
2. Dépliez le dossier **Cadres réglementaires**.
   La liste des **Types de risque** s'affiche.
3. Cliquez sur le bandeau du dossier **Types de risque**, sélectionnez **Nouveau > Type de risque.**



4. 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.*

   ☛ *Pour créer vos propres types de risque avec le profil **Risk Manager (simplifié)** : dans l'onglet **Bibliothèque des Risques**, sélectionnez **Risques > Catégories > Types de risque**.*

Les facteurs de risque

Beaucoup de facteurs de risque sont définis dans le cadre réglementaire international, national ou inter-professionnel, 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.*

Pour accéder à la liste des facteurs de risque avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et Risques**, puis dépliez le dossier qui correspond à votre référentiel.
   Les deux dossiers **Cadres réglementaires** et **Dispositifs de contrôle** apparaissent.
2. Dépliez le dossier **Cadres réglementaires**.
   L'arborescence des facteurs de risque apparaît.

On pourra 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.

☛ *Pour créer vos propres types de risque avec le profil **Risk Manager (simplifié)** : dans l'onglet **Bibliothèque des Risques**, sélectionnez **Risques > Catégories > Facteurs de risque**.*

Les types de contrôle

Les contrôles peuvent être définis en faisant référence aux types de contrôle définis dans le cadre du dispositif de contrôle et de risque concerné.

Une nomenclature de contrôles souvent utilisée est celle définie par le COBIT.

COBIT signifie "Control Objectives for Information and related Technologies".

COBIT est un cadre de meilleures pratiques qui vient intégrer les nombreux autres cadres et a le soutien d'un grand nombre d'experts mondiaux. Aux 34 processus définis par COBIT correspondent 318 objectifs de contrôle pour

lesquels des pratiques de contrôle détaillées ont été identifiées. Le guide de vérification proposé décrit les éléments nécessaires à la bonne compréhension de chaque processus, précise les contrôles à effectuer, fournit des éléments pour évaluer la conformité aux bonnes pratiques et évaluer le risque que les objectifs ne soient pas atteints.

📖 *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 accéder à la liste des types de contrôle avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et Risques**, puis dépliez le dossier qui correspond à votre référentiel.
   Les deux dossiers **Cadres réglementaires** et **Dispositifs de contrôle** apparaissent.
2. Dépliez le dossier **Cadres réglementaires**.
   L'arborescence des types de contrôle apparaît.

☛ *Pour créer vos propres types de risque avec le profil **Risk Manager (simplifié)** : dans l'onglet **Bibliothèque des Risques**, sélectionnez **Risques > Catégories > Types de contrôle**.*

Les acteurs externes : objectifs et exigences

📖 *Un acteur externe représente un organisme qui échange des flux avec l'entreprise. Ex : Client, Fournisseur, Administration.*

Définir les différentes parties concernées par les risques encourus par l'entreprise est important dans la majorité des activités. Cette analyse est généralement nécessaire dès les premières étapes d'un projet de gestion des risques.

Les *acteurs externes* à considérer peuvent être :

- Les législateurs
- Des agences gouvernementales, des ministères, ou des administrations locales.
- Des groupements d'intérêts tels que les lobbys écologistes
- Les services de secours d'urgence
- Les institutions financières et autres fournisseurs de fonds du secteur privé
- Les clients de l'organisation, y compris leur direction, leur encadrement et leur personnel
- Les fournisseurs et les sous-traitants
- Des personnes qui peuvent être affectées par les activités de l'entreprise du fait de leur proximité géographique
- Les médias

Pour accéder à l'ensemble des acteurs de l'organisation, voir "Acteurs internes de l'organisation", page 14.

Pour spécifier qu'un acteur est externe à l'organisation :

1. Ouvrez la fenêtre de propriétés de l'acteur et sélectionnez l'onglet **Caractéristiques**,

2. Dans le champ **Interne/Externe**, sélectionnez **Acteur externe**.
   Les **Acteurs externes** sont présentés avec une icône verte dans les diagrammes et dans les arbres de navigation.

CONTEXTE DE LA GESTION DES RISQUES

Le projet de gestion des risques doit être entrepris en prenant en compte parmi les objectifs de l'entreprise ceux qui sont pertinents pour ce projet. Il doit également considérer la nécessité d'équilibrer les coûts, les bénéfices et les opportunités.

> 🕮 *Un projet est une partie d'un système dont l'étude est confiée à une même équipe.*
>
> ☛ *Pour plus de détails sur les projets, voir "Les projets de gestion des risques", page 26.*

La responsabilisation des dirigeants vis-à-vis des risques pris par leur entreprise impose non seulement de mettre en place des dispositifs de contrôles permettant de maîtriser ces risques, mais aussi de pouvoir en faire la démonstration lors d'audits et de les rattacher aux paragraphes de la réglementation qui y correspondent.

Aux *dispositifs de contrôles* internes mis en place dans une entreprise peuvent se superposer des dispositifs de contrôles imposés par la réglementation (Loi Sarbanes-Oxley, etc.) ou par des clients (certification ISO 9000) ou encore des dispositifs de contrôle sectoriel (Bâle II dans le secteur bancaire, etc.).

> 🕮 *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 relatif à loi Informatique & Liberté, le dispositif de contrôle de gestion, le dispositif d'audit interne.*

Enfin, la description du contexte interne dans le cadre duquel se déroule le projet de gestion des risques peut être complétée par la description des *dispositifs de contrôle* existants.

A l'occasion d'un projet de gestion des risques, les dispositifs de contrôles existants vont être revus et de nouveaux *dispositifs de contrôle* peuvent être créés.

> ☛ *Pour plus de détails sur les dispositifs de contrôle, voir "Les dispositifs de contrôle", page 27.*

Les projets de gestion des risques

> 🕮 *Un projet est une partie d'un système dont l'étude est confiée à une même équipe.*

Le projet de gestion des risques doit être entrepris en prenant en compte parmi les objectifs de l'entreprise ceux qui sont pertinents pour ce projet. Il doit également considérer la nécessité d'équilibrer les coûts, les bénéfices et les opportunités.

Définir un projet de gestion des risques nécessite de :

- sélectionner les **objectifs** stratégiques et les exigences pertinents dans le cadre du projet,
- définir les **objectifs** spécifiques propres au projet,
- déterminer les ressources disponibles pour le projet (capital, acteurs, applications, …),
- sélectionner parmi les **dispositifs de contrôle** existants ceux qui sont concernés par le projet,
- définir les éventuels nouveaux **dispositifs de contrôle** à mettre en place,
- définir le périmètre du projet : acteurs, sites, processus et systèmes concernés, …

A l'occasion d'un projet de gestion des risques, les dispositifs de contrôles existants vont être revus et de nouveaux *dispositifs de contrôle* peuvent être créés.

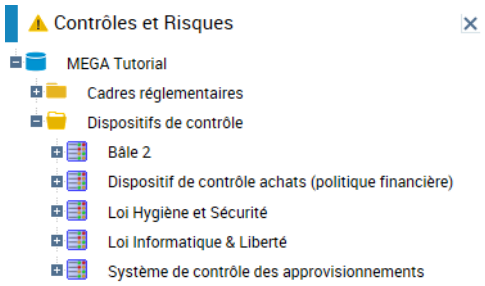
☛ *Pour plus d'information sur la gestion des projets, voir le guide **HOPEX Common Features**.*

Les dispositifs de contrôle

🕮 *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 relatif à loi Informatique & Liberté, le dispositif de contrôle de gestion, le dispositif d'audit interne.*

Pour accéder à la liste des dispositifs de contrôle avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et Risques**, puis dépliez le dossier qui correspond à votre référentiel.
   Les deux dossiers **Cadres réglementaires** et **Dispositifs de contrôle** apparaissent.
2. Dépliez le dossier **Dispositifs de contrôle**.
   La liste des dispositifs de contrôle définis dans la base apparaît.

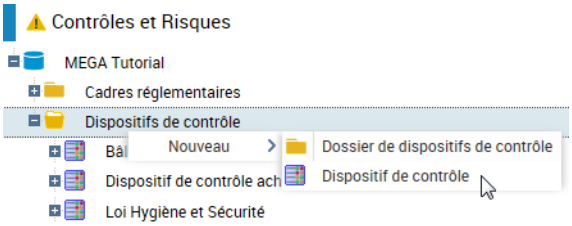


A chaque dispositif de contrôle peuvent être associés des *exigences*, des *types de risques*, etc.

Créer un dispositif de contrôle

Pour créer un dispositif de contrôle avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et risques**.
2. Dans le menu contextuel du dossier "Dispositifs de contrôle", sélectionnez **Nouveau > Dispositif de contrôle**.



Une fenêtre vous demande de saisir le nom du nouveau dispositif de contrôle.

3. Après avoir saisi le nom, cliquez sur **OK**.
   Le nouveau dispositif de contrôle apparaît dans l'arborescence du navigateur.

Caractéristiques d'un dispositif de contrôle

Pour accéder aux caractéristiques d'un *dispositif de contrôle* :

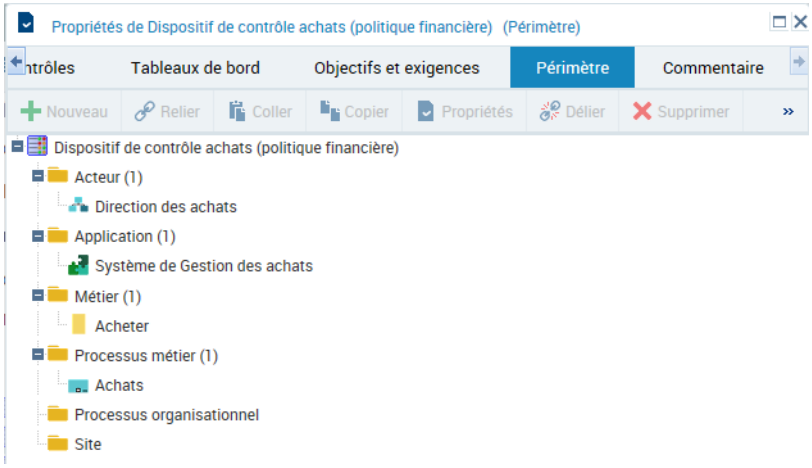
1. Ouvrez sa fenêtre de propriétés à l'aide de son menu contextuel.
2. Dans la fenêtre de propriétés qui s'ouvre, choisissez l'onglet **Caractéristiques**.

Vous pouvez saisir pour un dispositif de contrôle :

- Le **Code du dispositif de contrôle**
- La **Périodicité d'audit du dispositif de contrôle**.
- Le ou les **Cadres réglementaires** auxquels le dispositif de contrôle fait référence.

Périmètre d'un dispositif de contrôle

Dans l'onglet **Périmètre** de la fenêtre de propriétés du dispositif de contrôle, vous pouvez indiquez les *applications*, *métiers*, *processus*, *acteurs*, *sites*, etc. concernés par le dispositif de contrôle.



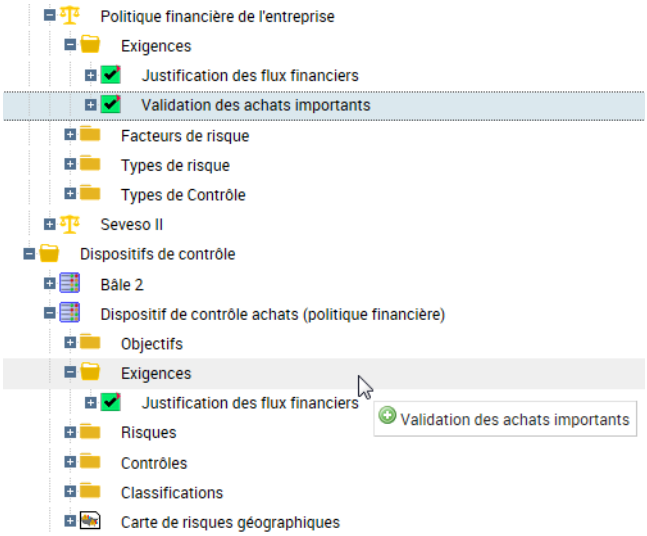
Exigences d'un dispositif de contrôle

> *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.*

Avec le profil ***Architecte Contrôle et Risques***, vous pouvez sélectionner, parmi les *exigences* associées aux *cadres réglementaires* auxquels le dispositif de contrôle fait référence, celles qui sont pertinentes pour ce *dispositif de contrôle*.

Pour cela :

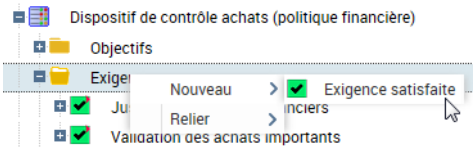
- Sélectionnez dans le navigateur les exigences qui vous intéressent et collez les dans le dossier "Exigences" du dispositif de contrôle.



Vous pouvez également rajouter des exigences spécifiques à ce dispositif de contrôle.

Pour créer une exigence avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Contrôles et risques**.
2. Dans le menu contextuel du dossier "Dispositifs de contrôle", sélectionnez **Nouveau > Exigence satisfaite**.



3. Saisissez son nom et cliquez sur **OK** pour faire apparaître cette nouvelle exigence dans la liste des exigences du dispositif de contrôle.

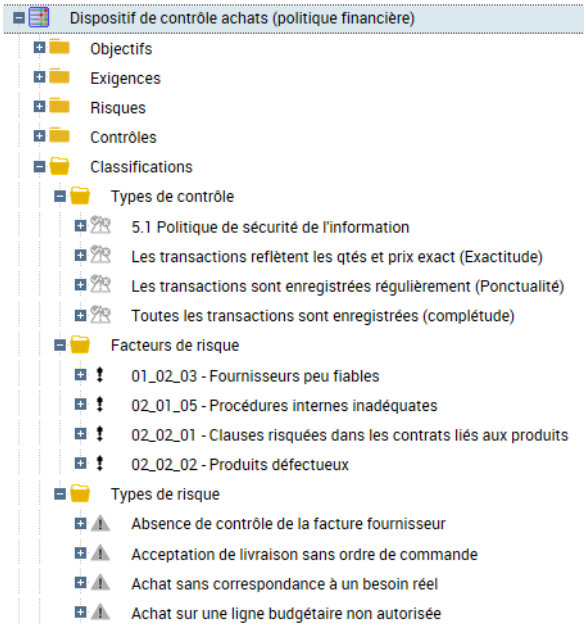
Objectifs du dispositif de contrôle

Vous pouvez retrouver les *objectifs* et les *exigences* du dispositif de contrôle dans l'onglet **Objectifs et Exigences** de sa fenêtre de propriétés.

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.

Classifications

Les différentes classifications (*facteurs de risques*, *types de risque*, *types de contrôle*) associées à un dispositif de contrôle sont accessibles depuis la fenêtre des propriétés du *dispositif de contrôle* et depuis le navigateur.



Comme pour les *exigences*, vous pouvez sélectionner parmi les classifications associées aux *cadres réglementaires*, celles qui sont pertinentes pour ce dispositif de contrôle.

ÉVALUER LES RISQUES

Pour maîtriser les risques, il faut pouvoir les évaluer. Il est par conséquent nécessaire d'identifier et de qualifier les risques encourus dans le déroulement d'un processus. Pour ce faire, **HOPEX Risk Mapper** permet de gérer la notion de risque.

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

L'entreprise se trouve confrontée à de nombreux types de risques : financiers, juridiques, écologiques, informatiques, techniques, commerciaux, contractuels, etc. Les décisions de traiter ou non chacun des risques peuvent être basées sur des critères opérationnels, techniques, financiers, légaux, sociaux, humanitaires, etc. Ces critères doivent refléter le contexte définit par le projet. Ils dépendent également de la politique interne de l'organisation, de ses objectifs et des intérêts de chacune des parties prenantes.

Le choix des méthodes d'évaluation et de traitement des risques doit être effectué en conformité avec les objectifs et les exigences du projet. La démarche de recherche et d'évaluation des risques peut combiner plusieurs approches complémentaires. Celles-ci peuvent être basées sur :

- ✓ l'atteinte des objectifs de l'entreprise,
- ✓ l'application de listes prédéfinies de types de risques, de facteurs de risques ou de types de contrôles à leur contexte d'apparition (processus, activité, etc.),
- ✓ des données historiques (bases d'incidents, de réclamations, de défauts…).

Dans **HOPEX Risk Mapper**, il existe différents types d'objets liés aux risques :

- les types d'objets pouvant encourir un risque (par exemple : *processus*, *application*, *opération*, *acteur*, etc.).
- les types d'objets permettant de traiter un incident ou de prendre des mesures préventives (*contrôle*, *processus*).

Les points suivants sont abordés ici :

IDENTIFIER LES RISQUES

Une fois que l'environnement interne de contrôle est défini et que les objectifs de l'entreprise en termes de risques ont été précisés, commence l'étape d'identification des événements à risque.

L'identification des risques est généralement effectuée dans le cadre d'un *dispositif de contrôle* déterminé.

> 🕮 *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 relatif à loi Informatique & Liberté, le dispositif de contrôle de gestion, le dispositif d'audit interne.*

Ce dispositif de contrôle peut être défini comme la mise en oeuvre d'une réglementation dans le cadre d'un des métiers de l'entreprise, comme par exemple, l'application de la politique financière de l'entreprise dans le domaine des achats.

Méthodes d'identification des risques

L'identification des événements à risque implique de recenser les événements internes et externes pouvant compromettre l'atteinte des objectifs. Une distinction doit être opérée entre ceux qui représentent des risques et ceux qui constituent des opportunités ou qui relèvent des deux simultanément. Les opportunités sont intégrées à la stratégie de l'organisation ou aux processus de fixation des objectifs.

La démarche d'identification des événements à risque peut se faire selon plusieurs approches qui associeront plus ou moins les opérationnels.

Méthode basée sur des listes de types de risques ou de facteurs de risques

Il est possible de commencer par définir une liste de risques génériques que l'on retrouve quelle que soit l'activité. Il s'agit en particulier des risques du type catastrophe naturelles, interruption de systèmes d'information, erreur humaine, fraude, etc.

Une première liste constituée par une équipe centrale, va permettre d'éviter de refaire un travail complet d'analyse des risques avec les opérationnels métiers pour se concentrer sur les risques spécifiques à leur activité. Cette liste pourra s'inspirer de textes réglementaires et de listes fournies par des partenaires de la profession (groupements interprofessionnels, compagnies d'assurances, etc.).

Cette liste pourra ensuite être complétée lors d'entretiens avec les opérationnels responsables des processus qui pourront définir à quels types de risques ils sont sensibles et en donner une définition précise.Dans ce cas, on identifie les processus et les diverses parties prenantes ou les acteurs de l'organisation concernés par ces types de risques ou ces facteurs de risques.

On établit pour chaque partie prenante un questionnaire spécifique d'identification des risques en sélectionnant parmi les types de risques ou facteurs de risques ceux qui peuvent la concerner.

Un questionnaire peut ainsi être réalisé et envoyé aux différentes parties prenantes pour leur permettre d'identifier les risques les concernant.

☛ *Voir le guide **HOPEX Assessment** pour plus d'informations sur les questionnaires.*

Des experts de chacun des sujets concernés analysent les réponses à ces questionnaires, avec éventuellement l'aide des acteurs concernés, pour finaliser l'identification des risques.

Il est possible ensuite de retirer de la liste générique, qui a été complétée par les risques spécifiques à l'activité, les événements à risque qui ne s'appliquent pas au domaine (ex : activité purement manuelle, ne faisant pas appel à un système d'information).

Méthode basée sur les objectifs de l'entreprise et la cartographie des processus

Il est possible de rechercher les risques de ne pas atteindre les objectifs d'une organisation ou de ne pas satisfaire les exigences réglementaires ou internes à cette organisation à partir de la description des processus de l'organisation.

On sélectionne pour cela les processus qui contribuent à l'atteinte de ces objectifs ou à la satisfaction de ces exigences. Puis on détermine les risques en analysant les flux échangés entre les acteurs qui interviennent dans ces processus, ainsi que les opérations réalisées par ces acteurs. On recherche parmi ces flux et ces opérations lesquels pourraient, en cas de mauvais fonctionnement, empêcher l'atteinte des objectifs ou la satisfaction des exigences de l'organisation.

Il est possible de compléter cette approche en s'appuyant sur d'autres critères d'identification des risques tels que des listes de types de risques ou de facteurs de risques quand ceux-ci sont disponibles.

Si une cartographie des processus de l'entreprise existe déjà, il est possible d'en tirer parti pour identifier les risques.

Les événements à risque peuvent être associés à chacun des processus modélisés.

Les risques associés à un processus sont visibles dans l'onglet **Risques** de la fenêtre de propriétés du processus.

☛ *Les risques peuvent être reliés à d'autres concepts tels que acteur, application, etc.*

Méthode d'identification à partir d'une base d'incidents

Il est possible d'utiliser toutes sortes d'enregistrements historiques, tels que des bases d'incidents, de défauts, de réclamations, etc.

Il s'agit d'analyser ces bases pour y découvrir des événements à risque. On précisera ensuite pour chaque risque ainsi découvert son contexte d'apparition (processus, acteur de l'organisation, application informatique, site de l'entreprise, etc.).

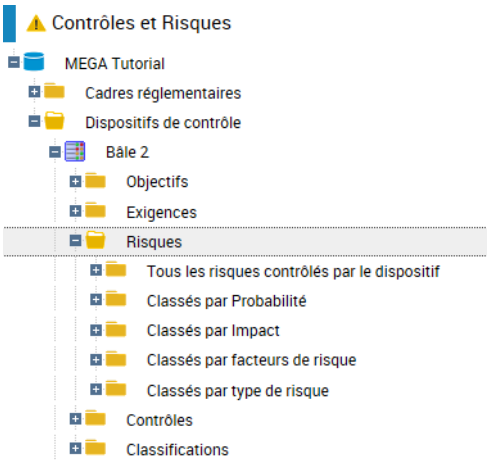
☛ *Voir le guide utilisateur **HOPEX LDC** pour plus d'informations sur la gestion des incidents.*

Accéder aux risques identifiés

Avec le profil ***Architecte Contrôle et Risques***, l'accès aux risques est possible à partir des dispositifs de contrôle.

Pour accéder aux risques avec le profil ***Architecte Contrôle et Risques*** :

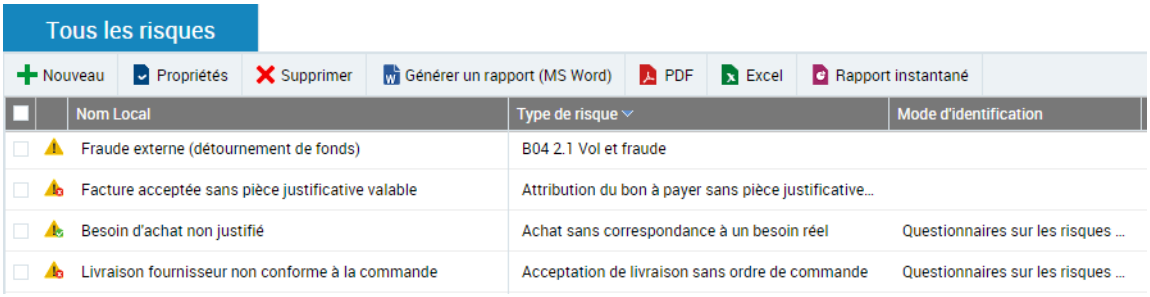
1. Cliquez sur **Contrôles et Risques > Dispositifs de contrôle.**
2. Sélectionnez un dispositif de contrôle et cliquez sur le dossier **Risques**.



☛ *Il est également possible de visualiser les risques couverts par un dispositif de contrôle à partir de l'onglet **Risques couverts** de la fenêtre de propriétés du dispositif de contrôle. Pour plus de détails, voir "Les dispositifs de contrôle", page 27.*

Pour accéder aux risques avec le profil ***Risk Manager (simplifié)*** :

- Cliquez sur **Bibliothèque des risques > Risques > Tous les risques**.



☛ *Pour accéder aux risques les risques les plus importants : Cliquez sur **Bibliothèque des risques > Risques > Risques clés**.*

Créer un risque

La procédure de création d'un risque varie en fonction du profil que vous utilisez.

Pour créer un risque associé à un processus organisationnel avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Objets principaux** puis dépliez le dossier **Processus métier**.
2. Ouvrez la fenêtre de propriétés du processus qui vous intéresse.
3. Cliquez sur l'onglet **Risques**.
4. Cliquez sur le bouton **Nouveau**.
   La fenêtre de création d'un risque apparaît.

Pour créer un risque avec le profil ***Risk Manager (simplifié)*** :

1. Cliquez sur l'onglet **Bibliothèque des risques** et sélectionnez **Risques > Tous les risques**.
2. Cliquez sur le bouton **Nouveau**.
   La fenêtre de création d'un risque apparaît.

Caractéristiques d'un risque

Dans la section **Caractéristiques** de la fenêtre de propriétés d'un risque vous pouvez préciser les caractéristiques suivantes :

- le **Code** d'identification du risque,
- le **Nom** du risque,
- le fait que le risque est de haut niveau en cochant éventuellement la case **Risque clé**,
- le **Propriétaire** du risque,

  ☛ *Par défaut, le **propriétaire** est le créateur 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. Pour plus de détails, voir le guide **HOPEX Enterprise Risk Management**.*

Le périmètre d'un risque

Le périmètre du risque permet de définir la localisation d'un risque. Il porte sur plusieurs types de composants :

- les **Processus métier** et des **Processus organisationnels** exposés au risque. Pour plus de détails, voir "Processus de l'organisation", page 16.

  🕮 *Un processus métier représente un système qui fournit des produits ou des services à un client interne ou externe à l'entreprise ou à l'organisation. Aux niveaux supérieurs, un processus métier définit une structuration et une catégorisation du métier de l'entreprise. Il peut être décomposé en d'autres processus. Le lien vers les processus organisationnels permet de décrire l'implémentation réelle du processus métier dans l'organisation. Un processus métier peut également être détaillé à l'aide d'une vue fonctionnelle.*

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

- les **Entités** concernées par le risque. Pour plus de détails, voir "Acteurs internes de l'organisation", page 14.

  🕮 *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 **Objectifs et exigences** attendus vis à vis de la gestion du risque. Pour plus de détails, voir "Objectifs et exigences de l'organisation",

page 15.

> *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.*

> *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.*

- les **Applications** : pour plus de détails, voir "Applications", page 17.

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

- 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.*

- les **Opérations**

  > *Une opération est une étape élémentaire d'un processus organisationnel correspondant à l'intervention d'un acteur de l'organisation.*

  > *Dans le produit **HOPEX Control and Risk**, un onglet **Situation** était proposé pour définir le périmètre d'un risque. Une option de compatibilité vous permet de reprendre les informations qui était définies dans cet onglet pour les intégrer au **Périmètre** du risque. Pour activer l'option de compatibilité, voir "Gérer les options relatives aux risques", page 22.*

Le RACI sur un risque

La page de propriétés d'un risque présente une section **RACI** pour définir les différentes personnes responsables de la gestion de ce risque.

> *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 Risk Mapper permet de préciser le niveau de responsabilité de différentes personnes :

- sur un risque,
- sur un contrôle.

Spécifier les responsabilités

Avec **HOPEX Risk Mapper**, les personnes sont représentées par des **personnes système**.

> 🕮 *Une personne système représente une personne de l'entreprise. Cette personne est peut être associée à un login et un rôle (ou un profil selon le mode de connexion). Le login donne accès à l'application HOPEX. Le rôle (ou le profil) définit les droits d'accès aux référentiels et aux fonctionnalités du produit. Une personne système, si elle est associée à un login, dispose, dans chaque référentiel, d'un bureau qui lui est propre auquel elle peut se connecter à partir de n'importe quel poste d'un environnement donné.*

Pour préciser les personnes responsables d'un objet :

1. Dans la page de propriétés de l'objet, dépliez la section **RACI**.
2. Reliez des personnes système dans chacun des onglets suivants :
   - **Réalisateur**
   - **Autorité**
   - **Consulté**
   - **Informé**.

> ☛ *Dans certaines solutions, les informations RACI peuvent être redondantes avec certains rôles définis par ailleurs dans la fenêtre de propriétés de l'objet ou au contraire les complètent.*

Par exemple, dans **HOPEX Enterprise Risk Management**, le réalisateur du processus est à spécifier directement dans le champ **Réalisateur** de la fenêtre de propriétés du processus et non pas dans la section RACI. Dans ce cas, il est en effet important de ne spécifier qu'un seul réalisateur.

ANALYSE DES RISQUES

L'analyse d'un risque a pour objectif d'obtenir une bonne compréhension de ce risque. Elle apporte des éléments permettant de décider si un traitement de ce risque est nécessaire et de choisir les stratégies de traitements les plus appropriées avec le meilleur rapport coût/efficacité. L'analyse du risque doit prendre en compte les sources du risque, ainsi que les conséquences positives ou négatives de ce risque.

La phase d'analyse aboutit à associer à un risque des :

- types de risque
- facteurs de risques (ou causes)
- des conséquences
- des objectifs.

La contextualisation d'un risque permet de classer les risques en fonction :

- de leur type, d'une part
- des objets sur lesquels ils portent, d'autre part.

Un même risque peut porter sur plusieurs types de composants spécifiés dans le périmètre du risque :

- une entité
- un processus
- une ligne métier
- un site.

> ☛ *Ces composants sont spécifiés dans les caractéristiques du risque, dans la section **Périmètre**. Pour plus de détails, voir "Le périmètre d'un risque", page 38.*

L'analyse d'un risque

Pour analyser un risque :

1. Sélectionnez un risque et ouvrez sa page de propriétés
2. Sous l'onglet **Caractéristiques**, dépliez la section **Analyse**.
   Un risque est caractérisé par :
   - Le ou les **Dispositifs de contrôle** qui prennent en charge la gestion de ce risque, voir "Les dispositifs de contrôle", page 27.
   - des **Types de risque**, pour plus de détails, voir "Les types de risque", page 22.

     > 🕮 *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", page 23.

     > 🕮 *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", page 42.

  📖 *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 **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.*

  ☛ *Voir le guide utilisateur **HOPEX LDC** pour plus d'informations sur la gestion des incidents.*

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.*

Pour définir les conséquences associées à un risque :

1. Ouvrez la fenêtre de propriété d'un risque et sélectionnez l'onglet **Caractéristiques**,
2. Ouvrez la section **Analyse**,
3. Sélectionnez l'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.*

Le diagramme causes/effets

L'analyse des risques les plus importants pourra être complétée à l'aide d'un diagramme cause-effets pour décrire l'enchaînement de ses causes et/ou de ses conséquences. Cette étude peut faire apparaître de nouveaux risques ou facteurs de risques.

Un diagramme Causes/Effets, aussi appelé "Diagramme d'Ishikawa" ou "Diagramme en arrête de poisson" permet de décrire un enchaînement de causes et de conséquences pour analyser une défaillance.

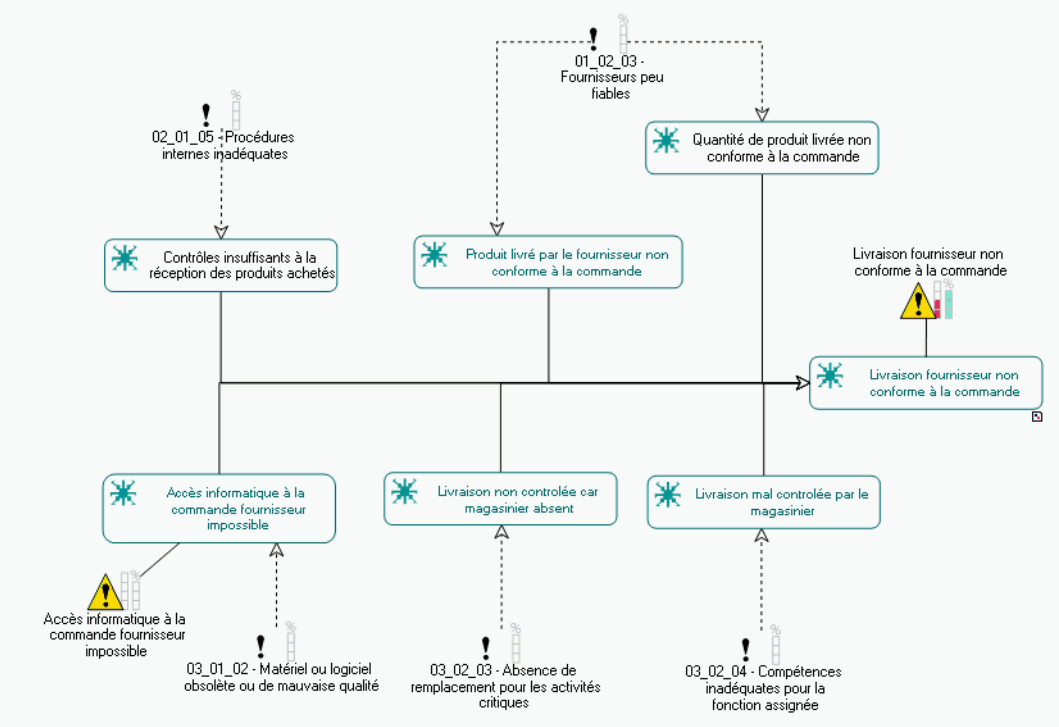


Diagramme Causes/Effets

Dans l'exemple ci-dessus, on analyse les causes possibles du risque "Livraison fournisseur non conforme à la commande".

On liste les causes possibles du problème, et pour chaque cause, on précise les facteurs de risques correspondants. A cette occasion, il est possible d'identifier de nouveaux risques.

☛ *Pour plus d'informations sur le diagramme Cause/Effets, voir le paragraphe "Le diagramme Causes/Effets" du chapitre "Objectifs et exigences" du guide **HOPEX Common Features**.*

☛ *Dans le guide **HOPEX Common Features**, défaillance et problème sont des notions équivalentes.*

EVALUER 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 Risk Mapper**, 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.

HOPEX Risk Mapper propose une possibilité d'évaluation directe qui permet à un expert de renseigner une évaluation globale d'un risque à une date donnée.

Si vous disposez de la solution **HOPEX Enterprise Risk Management** et que vous avez importé le framework associé, vous disposez de davantage de facilités d'évaluation.

☛ *Pour importer le framework, voir "Importer les bibliothèques spécifiques", page 21.*

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 "Les HeatMaps", page 69.

Evaluation directe des risques

L'évaluation directe permet de fournir, à une date donnée, une évaluation d'un risque sur une entité de l'organisation.

Vous pouvez effectuer :

- une évaluation directe à partir d'un risque
- une évaluation multiple à partir d'un tableau

Créer une évaluation directe

Vous pouvez créer de nouvelles évaluations en vue d'évaluer globalement un risque sur l'ensemble des objets de l'organisation auxquels il est relié (c'est-à-dire les entités).

Il s'agit d'une évaluation à dire d'expert.

Pour créer une évaluation :

1. Sélectionnez un risque et ouvrez sa page de propriétés
2. Cliquez sur l'onglet **Evaluation** du risque.
3. Cliquez sur le bouton **Evaluer**.
4. Sélectionnez les entités pour lesquelles le risque est à évaluer puis cliquez sur **Suivant**.

☛ *Les contextes sont proposés uniquement s'il en existe plusieurs.*

5. Renseignez les valeurs des caractéristiques :
   - **Impact** : impact du risque lorsqu'il se manifeste
   - **Probabilité** : probabilité que le risque se manifeste
   - **Niveau des contrôles**
6. Renseignez la date de l'évaluation.
7. Cliquez sur **OK**.
   Une évaluation est créée.

Représentation dans un diagramme

Pour afficher les risques avec leur probabilité et leur impact dans un diagramme :

- Cliquez sur **Affichages > Vues et détails** puis sélectionnez la vue "Risques".

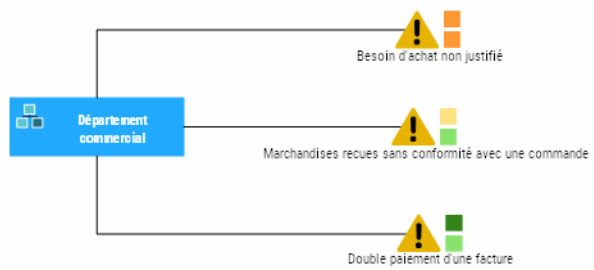
Dans la barre d'objets, le risque est représenté par un panneau "Danger" : 

Les couleurs placées à côté du panneau "Danger" varient en fonction des valeurs issues des évaluations du risque.

Impact: moyen, Probabilité : possible

Impact: très bas, Probabilité : possible

Les risques peuvent être affichés dans un diagramme avec les couleurs qui indiquent leur impact et leur probabilité.



Synthèse des risques

Heatmap par entité / type de risque / processus

Quand la probabilité et l'impact d'un risque ont été renseignés, il est possible d'obtenir une vue synthétique des risques afin de mettre en évidence les risques à traiter en priorité.

Pour cela, voir "Les HeatMaps", page 69.

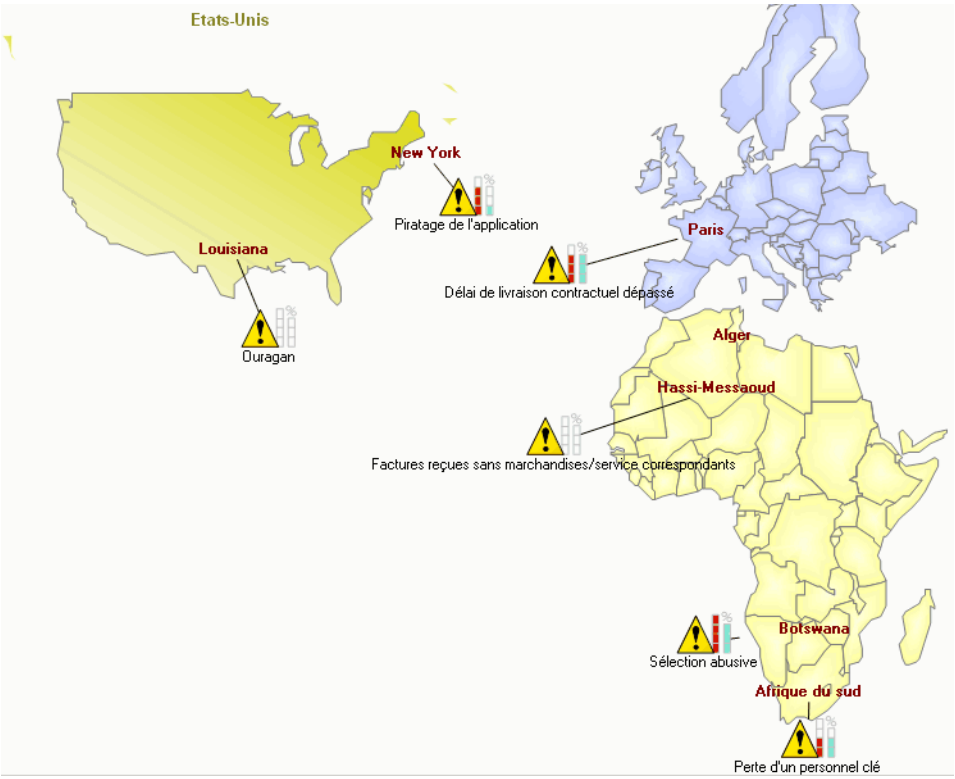
Carte géographique des risques

Il est également possible de décrire la répartition géographique des risques d'un dispositif de contrôle.

Pour cela :

- Créez une carte géographique des risques du dispositif de contrôle ou ouvrez-en une qui existe déjà.

La carte géographique des risques s'affiche.



Elle vous permet de relier les risques aux sites où ils peuvent se produire.

LE TRAITEMENT DES RISQUES ET LES CONTRÔLES

L'évaluation des risques a fourni une liste de risques pouvant nécessiter un traitement, avec leur estimation et un ordre de priorité.

Traiter les risques implique l'identification des différentes options possibles, l'évaluation de ces options ainsi que la préparation et la mise en oeuvre des plans de traitement.

Avant de déterminer les actions de traitement appropriées, il peut être utile de revoir l'analyse des risques et de l'étendre, pour en tirer les informations nécessaires à l'identification des différentes options de traitement. La conception des mesures de traitement des risques doit être basée sur une compréhension approfondie des risques concernés ; cette compréhension provient d'un niveau approprié d'analyse des risques. Il est particulièrement important d'identifier les causes des risques afin que ces risques soient traités et pas seulement leurs symptômes.

Il n'est généralement pas rentable, ni même désirable, de mettre en oeuvre tous les traitements possibles du risque. Il est cependant nécessaire de choisir et de mettre en oeuvre la combinaison de traitements du risque la plus appropriée.

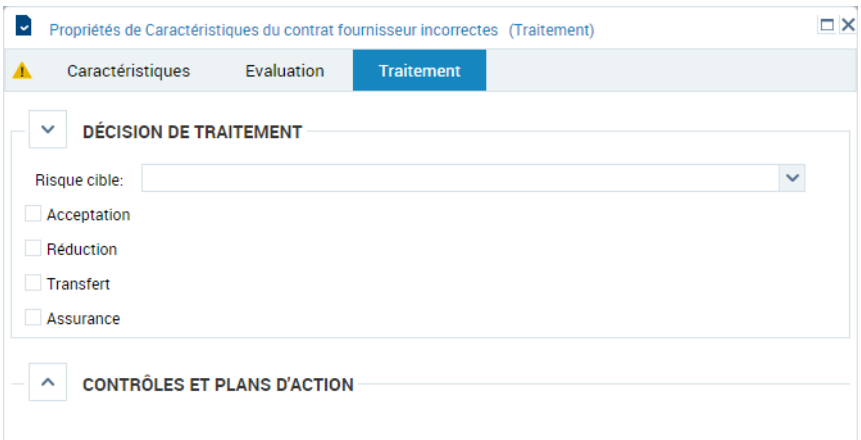
- ✓ "Le traitement du risque", page 50
- ✓ "Les contrôles", page 54

LE TRAITEMENT DU RISQUE

Une fois les risques analysés et évalués, le management détermine quels traitements appliquer à chacun de ces risques.

Pour spécifier les choix de traitement d'un risque :

- Ouvrez la fenêtre de propriétés du risque et sélectionnez l'onglet **Traitement**.



Choix du niveau de maîtrise des risques

Risque Cible

Pour un risque donné, il est possible de définir le niveau de risque acceptable pour l'organisation.

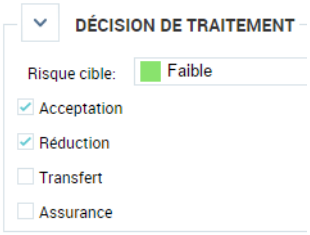
Le risque cible présente la valeur du risque résiduel attendue par le gestionnaire de risques après traitement du risque.

Si ce niveau de risque est supérieur ou égal au niveau risque évalué précédemment, l'organisation peut se contenter d'accepter le risque tel qu'il est.

Choix du niveau de maîtrise du risque

Pour chaque risque identifié, un niveau de risque acceptable pour l'organisation doit être défini.

Si le risque ne peut pas être accepté tel quel, diverses solutions permettant de faire face au risque peuvent être proposées.



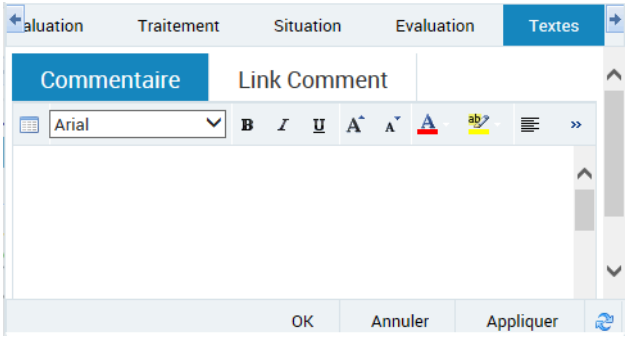
- ***Acceptation***
  Le risque est accepté et aucune action n'est mise en oeuvre pour essayer de le réduire.
- ***Réduction***
  Il est possible de réduire la probabilité du risque, en mettant en place des contrôles supplémentaires ou de réduire la gravité de ses conséquences si le risque survient.
- ***Transfert*** (sous-traitant)
  On peut également partager le risque avec d'autres partenaires, en particulier lorsque ceux-ci ont plus de compétences pour maîtriser le risque. Par exemple, on peut sous-traiter une activité dangereuse à un partenaire spécialisé dans ce domaine. Il faut noter que dans ce cas, il est souvent nécessaire de faire une nouvelle étude des risques car l'introduction d'un nouveau partenaire peut induire des risques supplémentaires.
- ***Assurance***
  En complément de toutes les approches précédentes, il est souvent nécessaire de recourir à une assurance, en particulier, pour les risques dont la probabilité est faible, mais la gravité élevé. Dans ce cas, l'assureur demandera généralement que des mesures de prévention et de réduction du risque soient également mises en place.

On analysera les différents scénarios possibles en mettant en regard leurs aspects positifs et négatifs, afin de choisir un scénario compatible avec le niveau de maîtrise du risque souhaité.

En fonction de la solution retenue, il convient de considérer l'effet des différentes solutions en termes de probabilité et d'impact ainsi que les coûts et bénéfices.

Le choix doit porter sur une solution ramenant le risque résiduel en déjà du seuil de tolérance souhaité par la direction.

Un commentaire vous permet de préciser le mode de traitement du risque.



Spécification des actions à mettre en oeuvre

Le management élabore un ensemble d'actions permettant de mettre en adéquation le niveau des risques avec le seuil de tolérance et l'appétence pour le risque de l'organisation.

Pour chaque risque, le scénario choisi est décrit en détail, en mettant en évidence les différents facteurs de risque et les contrôles mis en oeuvre pour les maîtriser. On précisera également quelles sont les contrôles mis en place pour prévenir le risque, ainsi que les processus curatifs à mettre en oeuvre si le risque survient.

Dans le cas d'un transfert vers des partenaires ou d'une assurance, on pourra préciser les contrats à établir avec eux, ainsi que l'impact prévisible sur les processus de l'organisation.

La mise en place de contrôles préventifs pour réduire la fréquence et l'impact du risque peut constituer une solution pour réduire le risque.

Pour indiquer les **Contrôles** et **Plans d'action** qui permettent de prévenir le risque :

- Dans l'onglet **Traitement** de la page de propriétés d'un risque, dépliez la section **Contrôles et plans d'action**.
  - L'onglet **Plans d'Action** dresse 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. Voir "Mise en place des plans d'action", page 53.

    Un plan d'action comprend une série d'actions. Son objectif est de réduire des risques ou des événements qui ont un impact négatif sur les activités de l'entreprise ou d'améliorer l'efficacité d'un processus ou d'une organisation.
  - L'onglet **Contrôles** dresse la liste des contrôles prévus pour réduire le risque. Voir "Contrôles préventifs du risque", page 53.

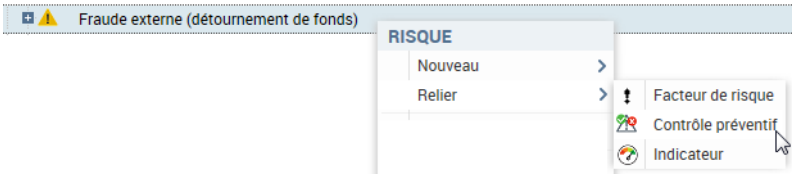
    Un contrôle est un moyen de maîtrise d'un ou plusieurs risques permettant de s'assurer qu'une exigence légale, réglementaire, stratégique ou interne à l'entreprise est respectée.

Contrôles préventifs du risque

La mise en place de contrôles préventifs pour réduire la probabilité et l'impact du risque peut constituer une solution pour réduire le risque.

Pour indiquer le ou les contrôles qui permettent de prévenir le risque:

- Cliquez sur le risque et sélectionnez **Relier > Contrôle préventif**.



☛ *Pour plus de détails sur la mise en oeuvre des contrôles, voir "Les contrôles", page 54.*

Mise en place des plans d'action

L'utilisation des plans d'action est disponible avec le produit **HOPEX Enterprise Risk Management**.

Un plan d'action comprend une série d'actions. Son objectif est de réduire des risques ou des événements qui ont un impact négatif sur les activités de l'entreprise ou d'améliorer l'efficacité d'un processus ou d'une organisation.

☛ *Pour plus de détails sur l'utilisation des plans d'action, voir le guide **HOPEX Enterprise Risk Management**.*

LES CONTRÔLES

Les activités de contrôle sont constituées des politiques et procédures qui permettent de s'assurer que les traitements des risques souhaités par la direction ont été effectivement mis en place. Les activités de contrôle sont présentes partout dans l'organisation, à tout niveau et dans toute fonction. Elles englobent un éventail d'activités aussi diverses que la validation, l'autorisation, la vérification, le rapprochement de données et la revue des performances opérationnelles, la sécurité des actifs ou la séparation des tâches.

L'identification et l'analyse des risques décrites précédemment ont permis de mettre en évidence un certain nombre de risques contre lesquels il est important de se prémunir. Il est alors nécessaire de définir les activités de contrôle qui vont permettre de prévenir ces risques et de diminuer leurs conséquences éventuelles.

Ces *contrôles* doivent être définis formellement pour pouvoir répondre aux exigences réglementaires telles que la loi Sarbanes-Oxley, ou les accords de Bâle II dans le monde bancaire.

> 🕮 *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.*

Dans **HOPEX Risk Mapper**, il existe différents types d'objets liés aux contrôles :

- les types d'objets permettant d'indiquer dans quel cadre ce contrôle est mis en place (*dispositif de contrôle*, *type de contrôle*, *exigence* ou *risque* associé)
- les types d'objets permettant d'indiquer les moyens de mise en oeuvre de ce contrôle (*processus*, *application*, *opération*, *service*, *contrainte* ou *ressource*, etc.).
- les types d'objets permettant d'indiquer les responsabilités dans la mise en oeuvre de ce contrôle (*acteur*, *personne*).

> ☛ *Les types d'objet opération et service sont disponibles avec le produit **HOPEX Business Process Analysis**.*

Identification des contrôles

Il est généralement préférable de recenser les contrôles existants avant d'en mettre en place de nouveaux.

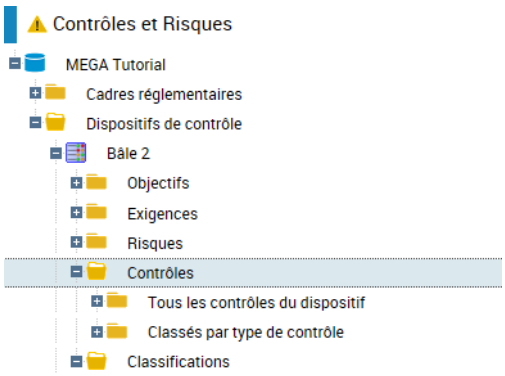
A cet effet, les contrôles peuvent être identifiés de différentes manières.

- à partir des risques
  Certains contrôles sont mises en place pour répondre à un risque particulier.
- à partir de listes de types de contrôles
  Des listes de types de contrôles sont associées à certaines réglementations (Ex: Cobit).
- à partir d'une cartographie des processus existants
  Comme pour identifier des risques, il est possible lorsque celle-ci est disponible d'examiner le fonctionnement de chacune des étapes d'un processus pour découvrir les contrôles mis en place.
- à partir de l'expertise d'un spécialiste
  Un spécialiste d'un domaine particulier est souvent capable de décrire les contrôles mis en place ou qui devraient l'être.
- à partir des bases d'incidents
  En consultant les événements passés, on peut proposer des contrôles qui auraient permis de les prévenir ou d'en diminuer les conséquences.

Accès aux contrôles

Pour accéder aux contrôles avec le profil ***Architecte Contrôle et Risques*** :

1. Cliquez sur **Contrôles et Risques > Dispositifs de contrôle.**
2. Sélectionnez un dispositif de contrôle et cliquez sur le dossier **Contrôles**.



☛ *Pour accéder aux contrôles avec le profil **Risk Manager (simplifié)** : dans l'onglet **Bibliothèque des risques**, sélectionnez **Contrôles > Tous les contrôles**.*

De même que les risques, les contrôles peuvent être très nombreux. Afin de mieux les maîtriser dans leur gestion, **HOPEX Risk Mapper** propose plusieurs critères de classification des contrôles.

☛ *Il est également possible de visualiser les contrôles couverts par un dispositif de contrôle à partir de l'onglet **Contrôles** de la fenêtre de propriétés du dispositif de contrôle. Pour plus de détails, voir "Les dispositifs de contrôle", page 27.*

Caractéristiques d'un contrôle

Dans l'onglet **Caractéristiques** de la page de propriété d'un contrôle, vous pouvez préciser :

- le **Code** permettant d'identifier le contrôle de manière unique.
- le **Nom** du contrôle
- le **Propriétaire** du contrôle

  ☛ *Par défaut, le **propriétaire** est le créateur du contrôle.*
- l'importance du contrôle en cochant éventuellement la case **Contrôle clé**
- le **Niveau**
- la **Nature de contrôle**
- le **Mode d'exécution**
- la **Fréquence**

Niveau du contrôle

Le niveau du contrôle permet de faire la distinction entre les contrôles "opérationnels" et les contrôles "organisationnels".

- niveau 1 : opérationnel
  Les contrôles de niveau opérationnel sont effectués lors du déroulement normal des processus de l'entreprise.
- niveau 2 : organisationnel
  Les contrôles de niveau organisationnel sont effectués par la suite et périodiquement par l'encadrement, pour vérifier que les processus opérationnels se sont bien déroulés et que leurs résultats sont conformes aux attentes.

Nature du contrôle

Cette caractéristique se rapporte aux motifs du contrôle :

- Correction,
- Détection,
- Prévention.

Mode d'exécution du contrôle

Cette caractéristique permet de préciser de quelle manière le contrôle est exécuté:

- Observation
- Contrôle par sondage
  Le contrôle est exécuté sur des échantillons prélevés au hasard.
- Contrôle systématique
  Le contrôle est exécuté systématiquement et de manière exhaustive sur tous les objets traités.

Fréquence d'exécution du contrôle

La périodicité d'exécution du contrôle peut être systématique, quotidienne, hebdomadaire, mensuelle, etc.

Le RACI sur un contrôle

La page de propriétés d'un contrôle présente une section **RACI** pour définir les différentes personnes responsables de la gestion de ce contrôle. Pour plus de détails, voir "Le RACI sur un risque", page 39.

Périmètre du contrôle

Vous pouvez définir de manière plus précise le contrôle en indiquant les risques, processus, entités et exigences qui lui sont rattachés.

Pour définir le périmètre du contrôle :

1. Ouvrez la page de propriétés d'un contrôle.
2. Dépliez la section **Périmètre**.
   Les onglets suivants sont disponibles :
   - les **Risques** couverts par les contrôles. Pour plus de détails, voir "Évaluer les risques", page 33.

     *Dans le produit **HOPEX Control and Risk**, un onglet **Risques prévenus** permet d'indiquer quels risques ou quels facteurs de risques sont prévenus par le contrôle. Une option de compatibilité vous permet de reprendre les informations qui était définies dans cet onglet pour les intégrer au **Périmètre** du contrôle. Pour activer l'option de compatibilité, voir "Gérer les options relatives aux risques", page 22.*
   - les **Processus métier** et des **Processus organisationnels** exposés aux risques couverts par le contrôle. Pour plus de détails, voir "Processus de l'organisation", page 16.
   - les **Entités** concernées par les contrôles. Pour plus de détails, voir "Acteurs internes de l'organisation", page 14.

Analyser un contrôle

Vous pouvez définir de manière plus précise le contrôle en indiquant les types de contrôle et dispositifs de contrôle qui lui sont rattachés.

Le(s) *types de contrôle* permettent de préciser le cadres réglementaires qui s'appliquent à un contrôle donné.

☛ *Pour plus de détails, voir "Les types de contrôle", page 23.*

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

Le dispositif de contrôle peut être défini comme la mise en œuvre d'une réglementation dans le cadre d'un des métiers de l'entreprise, comme par exemple l'application de la politique financière de l'entreprise dans le domaine des achats.

☛ *Pour plus de détails, voir "Les dispositifs de contrôle", page 27.*

Un dispositif de contrôle et de risque 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.

Objectifs et exigences d'un contrôle

L'onglet **Objectifs et exigences** permet d'indiquer à quel *objectif* de l'organisation ou à quelle *exigence* réglementaire ou légale répond le contrôle.

> 🕮 *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.*

> 🕮 *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.*

Mise en oeuvre d'un contrôle

Très souvent, la mise en place d'un contrôle consiste à vérifier qu'une règle de gestion (*contrainte*) est effectivement appliquée, que ce soit manuellement ou par un programme informatique.

> 🕮 *Une contrainte représente un contrôle ou une règle de gestion qui doit être appliquée lors de l'exécution d'un traitement.*

Vous pouvez spécifier les règles de gestion associées à un contrôle dans l'onglet **Règles de gestion** de la fenêtre de propriétés du contrôle.

Le contrôle peut être mis en oeuvre par :

- un *processus* : ce peut être le processus dans laquelle le contrôle est mis en oeuvre ou un processus préventif du risque (Ex : "Former les chargés de clientèle" pour prévenir le risque "Vente abusive"

  > 🕮 *Un processus métier représente un système qui fournit des produits ou des services à un client interne ou externe à l'entreprise ou à l'organisation. Aux niveaux supérieurs, un processus métier définit une structuration et une catégorisation du métier de l'entreprise. Il peut être décomposé en d'autres processus. Le lien vers les processus organisationnels permet de décrire l'implémentation réelle du processus métier dans l'organisation. Un processus métier peut également être détaillé à l'aide d'une vue fonctionnelle.*

- une *opération* : il s'agit de l'opération au cours de laquelle le contrôle est effectué

  > 🕮 *Une opération est une étape d'un processus correspondant à l'intervention d'un acteur de l'organisation dans le cadre d'une des activités de l'entreprise. Ce peut être une opération industrielle comme*

> _'usiner une pièce' ou logistique comme 'réceptionner une livraison', ou un traitement d'information comme 'enregistrer une commande'. Une opération peut être décomposée en Tâches élémentaires._

Il est possible de préciser le traitement qui va mettre en oeuvre le contrôle ou les règles de gestion associées au contrôle. Vous pouvez spécifier les moyens de mise en oeuvre du contrôle dans l'onglet **Caractéristique**, section **Périmètre.**.

SUIVI OPÉRATIONNEL DE LA POLITIQUE DE CONTRÔLE

Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques.

Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes, ou encore par une combinaison de ces deux modalités.

AMÉLIORATION CONTINUE DES DISPOSITIFS DE CONTRÔLE

Les dysfonctionnements identifiés par le suivi continu du fonctionnement opérationnel ou au cours des revues périodiques sont référencés et analysés. Les actions correctives sont ensuite planifiées et mises en oeuvre.

- Identification des dysfonctionnements
  Les dysfonctionnements à examiner sont identifiés à partir des différentes sources disponibles : le plan de traitement initial, les retours sur le traitement des risques et des incidents dans les dispositifs de contrôle en vigueur et les revues périodiques effectuées par les responsables opérationnels
- Analyse des dysfonctionnements
  Les dysfonctionnements sont étudiés pour en déduire les risques encourus par l'organisation. Ceux-ci sont ensuite analysés comme précédemment en déterminant les facteurs de risques et en s'aidant éventuellement d'un diagramme cause/effet.
- Mise en oeuvre du traitement des risques
  Après avoir déterminé les actions de traitement du risque à entreprendre, les besoins de conservation des données de contrôle, et les indicateurs de mesures des risques à mettre en oeuvre, un plan d'action comprenant les ressources nécessaires, les budgets, les échéances et les responsables de sa mise en oeuvre est défini.
- Suivi du plan d'action de traitement des risques
  La fréquence et les modalités du suivi du plan de traitement des risques sont établies.

Le référentiel **HOPEX** permet de définir les contrôles effectués lors du déroulement des processus de l'entreprise et de préciser par quels moyens organisationnels, informatique ou humain ils sont mis en oeuvre (voir "Le traitement des risques et les contrôles", page 49).

HOPEX vous permet également de décrire les procédures de remontée de l'information issue des contrôles effectués lors du déroulement des processus de l'entreprise (voir le guide **HOPEX Business Process Analysis**).

*Dans le produit **HOPEX Control and Risk**, un onglet **Redondance** permet d'indiquer que certains contrôles sont redondants. Une option de compatibilité vous permet d'utiliser cet onglet si nécessaire pour reprendre les informations qui était définies dans cet onglet afin de les intégrer au **Périmètre** du contrôle. Pour activer l'option de compatibilité, voir "Gérer les options relatives aux risques", page 22.*

EVALUATION DE L'EFFICACITÉ DES CONTRÔLES

En plus du suivi continu des risques lors du déroulement des processus de l'organisation, les responsables opérationnels effectuent des revues périodiques de la gestion des risques pour s'assurer que de nouveaux risques ne sont pas apparus et que les stratégies de traitement des risques appliquées sont toujours appropriées et efficaces. Pour ce faire, des questionnaires d'auto-évaluation des contrôles peuvent être utilisés.

En complément de ces revues par la hiérarchie opérationnelle, des audits internes ou externes à l'activité apportent une vue extérieure du fonctionnement de l'organisation et peuvent mettre en lumière de nouveaux dysfonctionnements.

Les découvertes des auditeurs vont généralement indiquer des faiblesses systématiques du système de maîtrise des risques. Les actions prises en réponse aux découvertes des auditeurs devront donc être focalisées sur des remèdes concernant le système dans son ensemble et non pas seulement sur les symptômes.

☛ *Pour plus de détails, voir le guide **HOPEX Internal Control**.*

SUIVI DES INCIDENTS ET DES PERTES

Après avoir mis en place une politique de traitement des risques, un suivi continu des risques encourus via la mesure régulière de différents paramètres (ex: niveaux de pollution, montant de la trésorerie disponible, etc.) doit être établi pour s'assurer de son bon fonctionnement.

Ceci peut être fait en particulier à partir de la gestion des bases d'incidents. Chaque incident y est répertorié et les pertes résultantes sont évaluées. Dans certains cas, on peut se contenter de s'assurer que l'activité de suivi des incidents est bien effectuée et qu'elle n'a pas produit de résultats dépassant les seuils de tolérance prévus.

Si de nouveaux risques sont identifiés à cette occasion, ils seront rajoutés à la liste des risques gérés par l'organisation. Les responsables opérationnels ou le responsable de la gestion des risques au sein de l'organisation devront les prendre en compte lors de la prochaine revue des risques.

☛ *Pour plus de détails, voir le guide **HOPEX LDC**.*

LES RAPPORTS HOPEX RISK MAPPER

HOPEX Risk Mapper offre des fonctionnalités d'analyse et de suivi des risques.

☛ *Pour plus de détails sur le fonctionnement des rapports, voir le chapitre "Générer des rapports" dans le guide **HOPEX Common Features**.*

Les différents types de rapports proposés en standard par **HOPEX Risk Mapper** visent à analyser les risques. Les types de rapports offrent différentes possibilités de présentation des analyses.

Les points suivants sont présentés dans ce chapitre :

LES RAPPORTS D'IDENTIFICATION

Matrice des risques encourus par les acteurs

Ce rapport recense les risques encourus par un ensemble d'acteurs.

☛ *Pour plus de détails sur la spécification des risques encourus par un acteurs, voir "Organiser les risques", page 12.*

Chemin d'accès

Pour accéder à ce rapport avec le profil ***Architecte Contrôle et Risques*** :

1. Cliquez sur l'acteur (ou le risque) qui vous intéresse et, à partir de son menu contextuel, sélectionnez **Recherche de rapport**.
   Un nouvel onglet **Rapports Disponibles** apparaît dans la fenêtre d'édition.
2. Ouvrez le dossier **Analyse des risques**.
   Le rapport **Matrice des risques encourus par les acteurs** dans la liste des rapports.
3. Cliquez sur le bouton **Personnaliser & Lancer un nouveau rapport** si vous souhaitez ajouter des acteurs ou des risques.

   ☛ *Lorsqu'un rapport type comprend plusieurs paramètres obligatoires, vous devez compléter le rapport avant de le lancer.*

   ☛ *Pour créer ce rapport avec le profil **Risk Manager (simplifié)** : dans l'onglet **Rapports**, sélectionnez **Identification > Matrice des risques encourus par les acteurs**.*

Paramètres du rapport

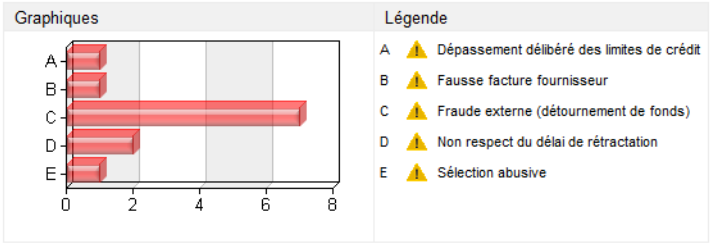
Paramètre	Type du paramètre	Contraintes
Acteurs exposés à des risques	Acteurs	Au moins un objet obligatoire.
Périmètre des risques analysés	Risque	Non obligatoire. Si aucune valeur n'est mentionnée, tous les risques sont analysés

Exemple de rapport

La première partie du rapport présente le nombre d'acteurs reliés à chacun des risque.

Dans l'exemple ci-dessous :

- un risque est relié à 7 acteurs
- un risque est relié à 2 acteurs
- trois risques sont reliés 1 seul acteur.



Nombre d'acteurs analysés:80

Nombre d'acteurs exposés aux risques:11

Ratio:13.8

La seconde partie du rapport présente la matrice des liens entre les acteurs et les risques qui font partie du périmètre et qui sont reliés entre eux.

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

	Dépassement délibéré des limites de crédit	Fausse facture fournisseur	Fraude externe (détournement de fonds)	Non respect du délai de rétractation	Sélection abusive
Agent Commercial	✓				✓
Acheteur		✓			
Compagnie aérienne			✓		
Direction Administrative et Financière				✓	
Direction commerciale				✓	
Acheteur			✓		
Assistant achats			✓		

Matrice des risques concernant les sites

Ce rapport recense les risques encourus par un ensemble de sites.

Il est identique au rapport "Matrice des risques encourus par les acteurs", page 66, seuls les paramètres varient.

Chemin d'accès

Pour accéder à ce rapport avec le profil ***Architecte Contrôle et Risques*** :

1. Cliquez sur l'acteur (ou le risque) qui vous intéresse et, à partir de son menu contextuel, sélectionnez **Recherche de rapport**.
   Un nouvel onglet **Rapports Disponibles** apparaît dans la fenêtre d'édition.
2. Ouvrez le dossier **Analyse des risques**.
   Le rapport **Matrice des risques concernant les sites** dans la liste des rapports.
3. Cliquez sur le bouton **Personnaliser & Lancer un nouveau rapport** si vous souhaitez ajouter des acteurs ou des risques.

   ☛ *Lorsqu'un rapport type comprend plusieurs paramètres obligatoires, vous devez compléter le rapport avant de le lancer.*

   ☛ *Ce rapport n'est pas proposé aux utilisateurs **Risk Manager (simplifié)**.*

Paramètres du rapport

Paramètre	Type du paramètre	Contraintes
Sites exposés aux risques	Sites	Au moins un objet obligatoire.
Périmètre des risques analysés	Risques	Non obligatoire. Si aucune valeur n'est mentionnée, tous les risques sont analysés.

LES HEATMAPS

HeatMap par entité / type de risque / processus

Ce rapport permet de visualiser la répartition des risques en fonction de différents critères :

- Impact du risque par rapport à sa probabilité d'occurrence
  - **Impact** : caractérise l'impact du risque lorsqu'il se manifeste
  - **Probabilité** : caractérise la probabilité que le risque se manifeste
- Risque brut par rapport au niveau des contrôles
  - **Risque brut** : est le produit de la valeur de l'impact par la valeur de la probabilité. Cette caractéristique donne un appréciation des conséquences du risque.
  - **Niveau de contrôle** : donne une appréciation globale du niveau de maîtrise du risque.

> ☛ *Pour plus de détails sur l'évaluation des risques, voir "Les évaluations avec HOPEX Enterprise Risk Management", page 17.*

Chemin d'accès

Pour accéder à ce rapport avec le profil ***Architecte Contrôle et Risques*** :

1. A partir du volet **Référentiel**, sélectionnez **Documentation** et dépliez le dossier **Rapports** et
2. Faite un clic droit **HeatMap par entité / type de risque / processus** et sélectionnez **Nouveau > Rapport**.
   Un nouvel onglet **Rapports Disponibles** apparaît dans la fenêtre d'édition.
3. Ouvrez le dossier **Analyse des risques**.
   Le rapport **HeatMap par entité / type de risque / processus** apparaît dans la liste des rapports.
4. Cliquez sur le bouton **Compléter**.

> ☛ *Lorsqu'un rapport type comprend plusieurs paramètres obligatoires, vous devez compléter le rapport avant de le lancer.*

> ☛ *Pour créer ce rapport avec le profil **Risk Manager (simplifié)** : dans l'onglet **Rapports**, sélectionnez **HeatMaps > HeatMaps par entité / Type de risque / Processus**.*

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.
Type de risque du contexte	type de risque	Critère de sélection des risques. Non obligatoire.
Entités du contexte	entité	Critère de sélection des risques. Non obligatoire.
Processus du contexte	processus	Critère de sélection des risques. Non obligatoire.
Objectifs du contexte	objectifs	Critère de sélection des risques. Non obligatoire.

Exemple de rapport

Dans l'exemple ci-dessous aucun risque n'a été évalué.

Impact /Probabilité

	Rare	Possible	Vraisemblable	Probable	Certain	
Trés élevé	0	0	0	0	0	0
Elevé	0	0	0	0	0	0
Moyen	0	0	0	0	0	0
Bas	0	1	0	0	0	1
Trés bas	0	2	0	1	0	3
Total	0	3	0	1	0	4

Niveau des contrôles /Risque inhérent

	Très bas	Bas	Moyen	Elevé	Très élevé	
Très faible	0	0	0	0	0	0
Faible	0	0	0	0	0	0
Moyen	0	3	0	0	0	3
Fort	0	1	0	0	0	1
Très fort	0	0	0	0	0	0
Total	0	4	0	0	0	4

☛ *Seules les dernières valeurs des évaluations de risques sont prises en compte pour chaque contexte Risque x Entité.*