HOPEX IT Risk Management

Guide d’utilisation

HOPEX V2

SOMMAIRE

Sommaire 1

Introduction à HOPEX IT Risk Management 7

Présentation de la solution 8
Processus 8
Gestion des risques informatiques 9
Gestion de la conformité informatique 9
Gestion des fournisseurs informatiques 9
Se connecter à HOPEX IT Risk Management 10
Conditions préalables 10
Lancer l'application 10
Les profils de la solution HOPEX IT Risk Management 10
Administrateur fonctionnel IT RM 11
IT RM Manager 11
Propriétaire d'application 12
Récapitulatif des droits par profil 12
Droits concernant les risques informatiques 12
Droits concernant la conformité informatique 13
Droits concernant les fournisseurs informatiques 13
Présentation de l'interface 14
A propos de ce guide 15
Structure du guide 15
Ressources complémentaires 15
Conventions utilisées dans le guide 16
Convention de formulation des commandes 16

Gérer les inventaires 17

Inventaire des actifs informatiques 18
A propos de l'inventaire des actifs informatiques 18
Intérêt de l'inventaire des actifs informatiques 18
Types d'actifs informatiques. 18
Accéder à l'inventaire informatique 19
Décrire les applications 19
Caractéristiques générales de l'application 19
Type d'une application 19
Périmètre fonctionnel de l'application 19
Responsabilités concernant une application 20
Technologies liées aux applications 20
Données échangées 21
Vulnérabilités d'une application 21
Contrôles reliés à une application 21
Décrire les technologies 21
Accéder aux technologies 21
Définir les caractéristiques d'une technologie 21
Types de technologie 22
Risques et vulnérabilités d'une technologie 22
Inventaire des menaces et vulnérabilités 23
Exemples de menaces, types de vulnérabilité et vulnérabilités 23
Consulter les menaces 23
Accéder aux menaces 23
Créer un type de menace 24
Caractéristiques des menaces 24
Consulter les vulnérabilités 24
Accéder aux vulnérabilités 24
Créer un type de vulnérabilité 24
Caractéristiques des vulnérabilités 25
Périmètre des vulnérabilités 26
Evaluation CVSS. 26
Rapports concernant les vulnérabilités 27
Inventaire des risques et contrôles 28
Consulter les risques 28
Accéder aux risques 28
Caractéristiques évaluées 28
Périmètre du risque 29
Analyse du risque 29
Evaluation du risque 29
Traitement du risque. 29
Consulter les contrôles 30
Accéder aux contrôles 30
Périmètre d'un contrôle 30
Evaluation de contrôles 30
Préparer l'environnement de travail pour les questionnaires 30
Inventaire des exigences et réglementations 32
Accéder aux exigences et réglementations 32
Caractéristiques des réglementations 32
Caractéristiques des exigences 32

Inventaire des fournisseurs 33
Accéder à la liste des fournisseurs 33
Caractéristiques des fournisseurs 33
Type de fournisseur 33
Liste des technologies fournies 33
Evaluation de risque fournisseur 34

Utiliser HOPEX IT Risk Management 35

Gérer les risques informatiques 36
Dresser l'inventaire informatique et identifier les vulnérabilités 36
Identifier les actifs informatiques 36
Positionner les vulnérabilités sur les actifs informatiques 36
Identifier et positionner les risques 37
Positionner les risques via une matrice 37
Positionner les risques individuellement sur chaque actif 37
Identifier les scénarios de risque 38
Créer un scénario de risque 38
Créer un diagramme de scénario de risque 38
Rapport de causalité de risques 40
Exemples 41
Evaluer les risques à dire d'expert 42
Evaluation directe des risques 42
Modèles d'évaluation des risques 43
Définir les plans d'action d'amélioration 43
Gérer la conformité informatique 44
Dresser l'inventaire des contrôles et types de contrôles 44
Liens entre Contrôles et Contrôles types 44
Relier les types de contrôles aux exigences réglementaires 45
Définir le périmètre applicatif du contrôle 45
Définir les exigences réglementaires à respecter 45
Identifier les contrôles sur les applications 46
Evaluer les contrôles à dire d'expert 46
Evaluer directement les contrôles 46
Modèle utilisé pour l'évaluation des contrôles 47
Gérer les fournisseurs informatiques 48
Identifier les fournisseurs informatiques 48
Spécifier le coût des produits et services 48
Evaluer les fournisseurs 49

Evaluations par questionnaires 51

Principe de l'évaluation par campagnes 52
Présentation des concepts 52
Session d'évaluation 52
Questionnaire 52

Campagne d'évaluation *52*
Etapes de l'évaluation 52
Préparer l'environnement de travail *52*
Lancer une campagne et ses sessions d'évaluation *53*
Créer une campagne d'évaluation **54**
Accéder aux campagnes d'évaluation 54
Créer une campagne d'évaluation 54
Créer une session d'évaluation **55**
Accéder aux sessions d'évaluation 55
Créer une session d'évaluation 55
Créer une session d'évaluation *55*
Prévisualiser les paramètres de la session d'évaluation *56*
Créer et lancer une session d'évaluation *56*
Planifier les sessions au sein de la campagne (facultatif) **57**
Déployer une campagne d'évaluation 57
Définir le périmètre de la campagne d'évaluation et les répondants 58
Définir le périmètre de la campagne d'évaluation *58*
Spécifier les répondants *58*
Répartir les évaluations au sein des différentes sessions 58
Valider la campagne d'évaluation **60**
Visualiser les objets à évaluer et leurs contextes **61**
Définir le périmètre de la session et les répondants **62**
Définir le périmètre de la session 62
Spécifier les répondants 62
Valider les objets à évaluer et leur contexte **63**
Valider la session d'évaluation 63
Visualiser les questionnaires générés 63
Re-générer les questionnaires 64
Envoyer les questionnaires **65**
Remplir les questionnaires **66**
Accéder aux questionnaires d'évaluation 66
Demander le transfert d'un questionnaire 66
Suivre l'avancement des questionnaires **68**
Consulter les résultats de la session 68
Visualiser les questionnaires envoyés 68
Valider les questionnaires d'évaluation 68
Demander à un répondant de modifier ses réponses 68
Réassigner un questionnaire 69
Fermer la session d'évaluation **71**

Traiter les risques **73**

Mode de traitement des risques **74**
Modes de traitement 74
Niveaux de risque *74*
Spécifier les contrôles et actions à mettre en œuvre 75

Gérer les plans d'action 76
Créer un plan d'action 76
Caractériser le plan d'action 76
Caractéristiques générales 77
Analyse financière 77
RACI 78
Facteurs de succès. 78
Périmètre 78
Jalons. 78
Pièces jointes 78
Gérer les actions 78
Workflows des plans d'action 79
Approche "bottom-up" 79
Approche "top-down" 79
Workflow des actions 80
Suivre les plans d'action 80
Renseigner l'avancement d'un plan d'action 80
Rapports de suivi des plans d'action. 80

Rapports de HOPEX IT Risk Management 83

Accéder aux rapports 84
Accéder à l'onglet dédié aux rapports. 84
Accéder aux rapports disponibles directement sur les objets 84
Accéder aux widgets 84
Rapports concernant les risques informatiques. 86
Rapports concernant l'identification des risques 86
Criticité des applications 86
Tableau Menaces et Vulnérabilités 87
Rapports concernant les actifs informatiques 88
Niveau de risque agrégé par processus métier 88
Heatmap des risques 89
Heatmap des applications 91
Widgets concernant les risques 92
Rapport de causalité de risques 94
Rapports concernant les vulnérabilités 94
Rapports concernant la conformité informatique. 97
Identification des contrôles 97
Chemin d'accès 97
Paramètres 98
Résultat 98
Exemple 98
Niveau de contrôle par réglementation 99
Chemin d'accès 99
Paramètres 100
Résultat 100
Exemple 101
Niveau de contrôle par processus métier. 101
Chemin d'accès 101

Paramètres *101*
Résultat *101*
Exemple *102*
Widgets concernant la conformité 102
Conformité des processus *102*
Conformité réglementaire *103*
Niveau de contrôle global *103*
Rapports concernant la gestion des fournisseurs 105
Matrice Fournisseur par type x Niveau de risque 105
Chemin d'accès *105*
Paramètres *105*
Résultats *105*
Exemple *105*
Niveau de risque fournisseur par ligne métier 106
Chemin d'accès *106*
Paramètres *106*
Résultats *106*
Exemple *106*
Rapports concernant les évaluations 107
Suivi des sessions 107
Chemin d'accès *107*
Paramètres *107*
Résultat *107*
Statistiques des sessions 107
Chemin d'accès *107*
Paramètres *108*
Résultat *108*

Annexe - Workflows 109

Workflow des évaluations 110
Workflow générique d'une campagne d'évaluation 110
Workflow générique d'une session d'évaluation 111
Workflow générique des questionnaires 111
Workflow des plans d'action 113
Workflow de plan d'action "top-down" *113*
Workflow de plan d'action "bottom-up" *114*
Workflow d'une action *115*

INTRODUCTION

Chaque entreprise doit mettre en place des processus de gouvernance et de gestion des technologies de l'information.

HOPEX IT Risk Management permet de définir et d'automatiser un système de gouvernance approprié. Cette solution permet d'analyser les risques à partir de l'architecture informatique actuelle et de définir le niveau de contrôle requis pour remplir les objectifs de l'entreprise. **HOPEX** s'attache plus particulièrement à construire un environnement de contrôle adéquat supportant les processus de l'entreprise.

La solution s'adresse aux départements informatiques, et plus particulièrement aux départements de gestion des risques, de conformité, de sécurité informatiques.

- ✓ "Présentation de la solution", page 8
- ✓ "Se connecter à HOPEX IT Risk Management", page 10
- ✓ "Présentation de l'interface", page 14
- ✓ "A propos de ce guide", page 15

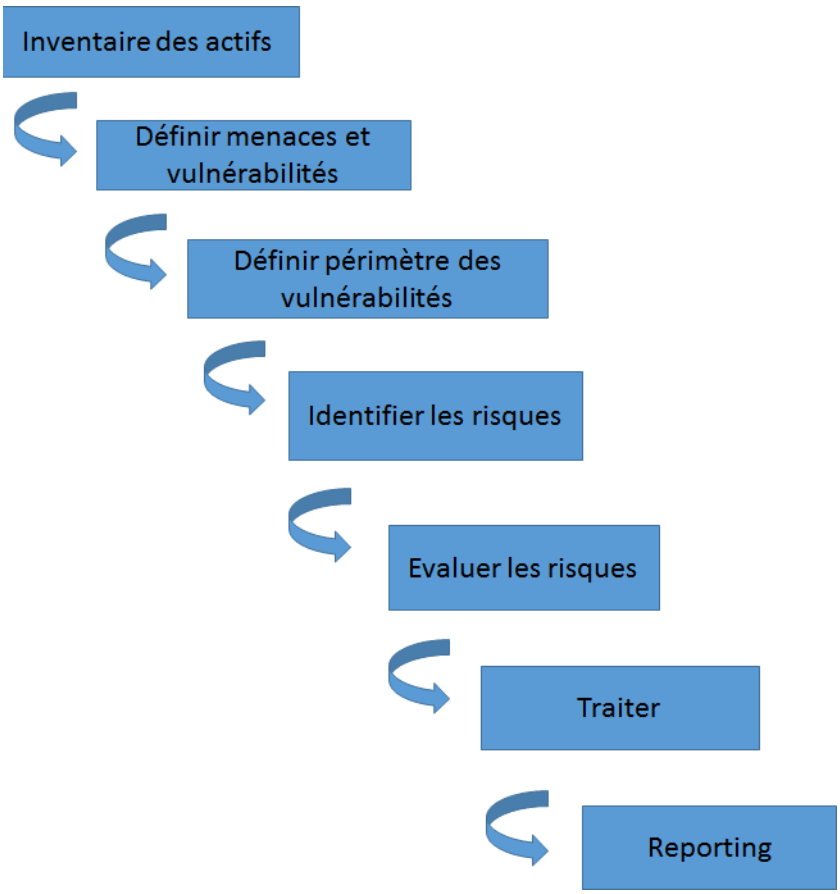
Voici les points abordés dans **HOPEX IT Risk Management** :

- ✓ "L'environnement des solutions HOPEX", page 501
- ✓ "Gérer les inventaires", page 17
- ✓ "Utiliser HOPEX IT Risk Management", page 35
- ✓ "Evaluations par questionnaires", page 51

PRÉSENTATION DE LA SOLUTION

HOPEX IT Risk Management permet de gérer les risques, la conformité et les fournisseurs informatiques. Vous pouvez capitaliser sur les inventaires hérités de **HOPEX Architecture** ou **HOPEX IT Portfolio Management**, ou les saisir directement dans la solution.

Processus



Gestion des risques informatiques

HOPEX IT Risk Management permet :

- d'identifier les menaces et vulnérabilités en se basant sur des frameworks ou sources d'informations appropriés (par exemple : ISO 27005, CVE).
- de produire des rapports concernant les vulnérabilités et d'identifier les risques menaçant les actifs informatiques.
- d'évaluer le niveau de risque des actifs informatiques à dire d'expert ou via des questionnaires envoyés aux propriétaires d'application.
- d'identifier les scénarios de risque et les liens de cause à effet entre risques.

Gestion de la conformité informatique

Les département informatiques doivent se conformer à un certain nombre d'exigences réglementaires et déployer en conséquence différents types de contrôles sur les actifs informatiques.

HOPEX IT Risk Management permet :

- d'identifier les cadres réglementaires informatiques appropriés (ISO 27002, NIST), les exigences qui en découlent ainsi que les types de contrôles à mettre en œuvre.
- d'évaluer le niveau de contrôle (conception et efficacité du contrôle) à dire d'expert ou via des questionnaires envoyés aux propriétaires d'application.
- produire des rapports illustrant le niveau de conformité réglementaire atteint.

Gestion des fournisseurs informatiques

HOPEX IT Risk Management permet :

- de saisir les données commerciales du fournisseur
- de lancer des campagnes d'évaluation dans le but d'évaluer la relation avec ces fournisseurs
- d'évaluer le niveau de risque global du fournisseur

SE CONNECTER À HOPEX IT RISK MANAGEMENT

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

Lancer l'application

Pour se connecter à **HOPEX IT Risk Management**, voir HOPEX Common Features, "Le bureau HOPEX", "Accéder à HOPEX (Web Front-End)".

Les profils de la solution HOPEX IT Risk Management

Dans **HOPEX IT Risk Management**, il existe, par défaut, des profils auxquels sont associées des activités spécifiques.

> ☛ *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.*

Administrateur fonctionnel IT RM

L'administrateur fonctionnel IT RM (IT Risk Management) gère essentiellement les objets de l'environnement (organisation, processus, capacité métier, ligne métier et inventaire des actifs informatiques).

> ☛ *L'inventaire applicatif peut également avoir été constitué au préalable via **HOPEX Architecture** ou **HOPEX IT Portfolio Management** par les gestionnaires de portefeuille applicatif et d'application.*

Il a accès aux bureaux suivants :

- **Administration**

  > ☛ *Pour plus de détails sur ce bureau, voir le guide **HOPEX Administration - Supervisor,** chapitre "Accéder à MEGA Administration".*

- **Environnement**

  > ☛ *pour plus de détails, voir "L'environnement des solutions HOPEX", page 501.*

- **IT RM**

Ses tâches principales sont les suivantes :

- il dresse l'inventaire applicatif
- il dresse l'inventaire des prestataires et éditeurs
- il assigne chaque application à un ou plusieurs IT RM Manager
- il assigne éventuellement les applications à des processus et/ou lignes métiers

IT RM Manager

Les managers IT RM (IT Risk Management) sont les principaux utilisateurs de la solution **HOPEX IT Risk Management**.

Ils peuvent appartenir à plusieurs départements (sécurité, conformité, gestion des risques).

Ils possèdent l'ensemble des droits sur les menaces, vulnérabilités, risques, contrôles, objets de l'évaluation, réglementations, exigences et rapports.

Ses tâches principales sont les suivantes :

- établir l'inventaire des menaces et vulnérabilités
- identifier les vulnérabilités sur chaque actif
- positionner les risques sur les actifs informatiques
- évaluer les risques
- décrire les plans d'action et d'amélioration

- identifier les exigences réglementaires
- identifier les contrôles
- évaluer les contrôles
- évaluer la conformité réglementaire

- saisir le coût annuel des produits ou services par fournisseur
- faire une évaluation du fournisseur

Propriétaire d'application

Le propriétaire d'application répond aux questionnaires qu'il reçoit dans le cadre des campagnes d'évaluation.

Il peut également prendre en charge les plans d'action qui lui sont confiés.

Récapitulatif des droits par profil

Droits concernant les risques informatiques

Pour plus de détails, voir "Gérer les risques informatiques", page 36.

	Administrateur fonctionnel IT RM	IT RM Manager
Dresser l'inventaire applicatif Voir "Inventaire des actifs informatiques", page 18.	X	
Dresser l'inventaire des menaces et vulnérabilités Voir "Inventaire des menaces et vulnérabilités", page 23.	X	X
Identifier les vulnérabilités sur chaque actif Voir "Positionner les vulnérabilités sur les actifs informatiques", page 36.	X	X
Identifier et évaluer les risques liés aux actifs informatiques Voir "Identifier et positionner les risques", page 37, "Evaluer les risques à dire d'expert", page 42.	X	X
Identifier les scénarios de risque Voir "Identifier les scénarios de risque", page 38.	X	X
Définir les plans d'action d'amélioration Voir "Traiter les risques", page 73.	X	X

Droits concernant la conformité informatique

Pour plus de détails, voir "Gérer la conformité informatique", page 44

	Administrateur fonctionnel IT RM	IT RM Manager
Identifier les contrôles Voir "Identifier les contrôles sur les applications", page 46	X	X
Évaluer l'efficacité des contrôles Voir "Evaluer les contrôles à dire d'expert", page 46	X	X

Droits concernant les fournisseurs informatiques

Pour plus de détails, voir "Gérer les fournisseurs informatiques", page 48

	Administrateur fonctionnel IT RM	**IT RM Manager**
Dresser l'inventaire des prestataires et éditeurs Voir "Inventaire des fournisseurs", page 33.	X	
Spécifier le montant annuel des achats Voir "Spécifier le coût des produits et services", page 48.	X	X
Évaluer les fournisseurs (attribution d'un score) Voir "Evaluer les fournisseurs", page 49	X	X

PRÉSENTATION DE L'INTERFACE

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

> ☛ *Pour plus de détails sur les profils, voir "Les profils de la solution HOPEX IT Risk Management", page 10 et "Récapitulatif des droits par profil", page 12.*

Les onglets de navigation reprennent les différentes phases de gestion des risques informatiques :

- **Inventaires**
  Voir "Gérer les inventaires", page 17
- **Campagnes d'évaluation**
  Voir "Evaluations par questionnaires", page 51
- **Traitement**
  Voir "Traiter les risques", page 73
- **Rapports**
  Voir "Rapports de HOPEX IT Risk Management", page 83

L'onglet **Accueil** vous permet d'accéder aux objets qui sont sous votre responsabilité.

Un tableau de bord composé de widgets vous permet d'accéder à une synthèse des informations contenues dans le référentiel. Pour plus de détails, voir "Accéder aux widgets", page 84.

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

A PROPOS DE CE GUIDE

Ce guide présente les fonctionnalités de la solution **HOPEX IT Risk Management**.
Il suit les grandes étapes suivantes :

- Établir l'inventaire des actifs informatiques
- Définir les menaces et vulnérabilités
- Identifier les risques
- Évaluer les risques
- Traiter les risques
- Reporting

> ☛ *Les fonctionnalités de reporting sont disponibles à tout moment, de manière globale, ou pour chaque étape du processus.*

Structure du guide

Ce guide est composé des chapitres suivants :

✓ "L'environnement des solutions HOPEX", page 501, décrit les différents éléments de l'environnement utilisés dans les solutions **MEGA**.

✓ "Gérer les inventaires", page 17, décrit l'inventaire des actifs informatiques, menaces et vulnérabilités, risques et contrôles, fournisseurs.

✓ "Utiliser HOPEX IT Risk Management", page 35, décrit les différents cas d'utilisation de la solution, à savoir la gestion des risques informatiques, de la conformité et des fournisseurs.

✓ "Evaluations par questionnaires", page 51, décrit les étapes nécessaires à l'envoi de questionnaires dans le cadre de campagnes d'évaluation

✓ "Traiter les risques", page 73, décrit comment traiter les risques et gérer les plans d'action.

✓ "Glossaire", page 25

✓ "Annexe - Workflows", page 109

Ressources complémentaires

Ce guide est complété par :

- le guide **HOPEX Common Features**, qui décrit l'interface MEGA.

  > ☛ *Il peut être utile de consulter ce guide pour une présentation générale plus détaillée de l'interface.*

- le guide d'administration **HOPEX Power Supervisor**.

Conventions utilisées dans le guide

☛ *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.

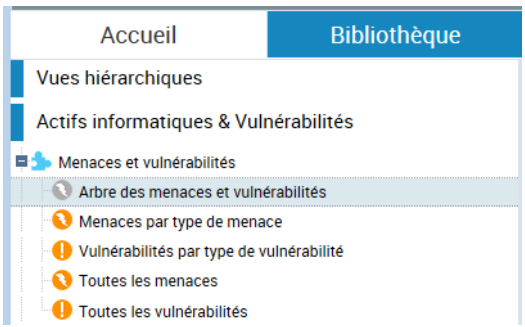
Remarque très importante à prendre en compte pour ne pas commettre d'erreurs durant une manipulation.

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

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

Convention de formulation des commandes

Pour faire référence à une commande dans la solution, et par souci de simplification, la formulation suivante a été adoptée dans le guide :

Commande de l'application	Formulation adoptée dans le guide
	Cliquez sur **Bibliothèque > Actifs informatiques et vulnérabilités > Menaces et Vulnérabilités > Arbre des menaces et vulnérabilités**.

Exemple de commande avec sa formulation dans le guide

GÉRER LES INVENTAIRES

Les inventaires IT RM (IT Risk Management) permet de consulter et de dresser l'inventaire des éléments nécessaires à la gestions des risques, de la conformité et des fournisseurs informatiques.

✓ "Inventaire des actifs informatiques", page 18
✓ "Inventaire des menaces et vulnérabilités", page 23
✓ "Inventaire des risques et contrôles", page 28
✓ "Inventaire des exigences et réglementations", page 32
✓ "Inventaire des fournisseurs", page 33

☛ *Pour plus de détails sur les cas d'utilisation des inventaires, voir "Utiliser HOPEX IT Risk Management", page 35*

INVENTAIRE DES ACTIFS INFORMATIQUES

A propos de l'inventaire des actifs informatiques

Un actif informatique est un artefact logiciel (ex : application, technologie logicielle) ou matériel (ex : site, serveur) détenu par l'entreprise et utilisé dans le cadre de ses activités.

Il existe deux "familles" d'actif informatique :

- Actif informatique (Type)

  ☛ *Un type d'actif est une catégorie spécifique d'actif informatique regroupant les types d'objets (Application, Technologie logicielle, etc.), par opposition aux objets déployés (instances).*

- Actif informatique (Instance)

  ☛ *Une instance d'actif est un type spécifique d'actif informatique regroupant les objets du déploiement (installation logicielle et technologie déployée).*

Intérêt de l'inventaire des actifs informatiques

La première partie de la gestion des actifs informatiques consiste à identifier et à décrire les actifs informatiques de votre entreprise. Ce n'est que lorsque vous avez découvert tous les actifs que vous pouvez les contrôler et les gérer efficacement.

La gestion des actifs informatiques est essentielle, tant en terme financier qu'en terme opérationnel. En effet, une bonne gestion permet d'optimiser les ressources, ainsi que de limiter les risques liés à la conformité et à la sécurité.

Types d'actifs informatiques

Un type d'actif informatique est une catégorie d'actif regroupant les types d'objets (Application, Logiciel, Technologie), par opposition aux objets déployés appelés instances.

Il est possible de distinguer :

- les Actifs
  - Application

    ☛ *Une application métier est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques et des fonctionnalités fournies aux utilisateurs.*

  - Technologie

    ☛ *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

- les Actifs déployés :
  - Installation logicielle

    ☛ *Une installation logicielle représente le déploiement d'une application en vue de son utilisation sur un site donné.*

  - Technologie déployée

Accéder à l'inventaire informatique

Pour accéder à l'inventaire informatique de l'entreprise :

- Dans le menu de navigation principal, cliquez sur **Inventaires**.

Voir :

- "Décrire les applications", page 19
- "Décrire les technologies", page 21
- "Inventaire des menaces et vulnérabilités", page 23
- "Inventaire des risques et contrôles", page 28
- "Inventaire des exigences et réglementations", page 32
- "Inventaire des fournisseurs", page 33

Décrire les applications

Pour accéder aux caractéristiques qui permettent d'identifier une application :

- Dans les pages de propriétés d'une application, cliquez sur **Caractéristiques**.

Caractéristiques générales de l'application

Vous pouvez spécifier :

- le **Nom** de l'application
- le **Code** interne

Type d'une application

Les technologies peuvent être de plusieurs types :

- bureautique
- développement spécifique
- middleware
- progiciel
- système

Périmètre fonctionnel de l'application

Pour consulter les objets qui définissent la couverture fonctionnelle d'une application :

- Dans les pages de propriétés de l'application, cliquez sur **Caractéristiques** puis sur **Périmètre fonctionnel**.

Les types de données qui définissent la couverture fonctionnelle de l'application sont :

- Les lignes métier qui utilisent l'application

  Une ligne métier est un haut niveau de classification des principales activités de l'entreprise. Elle correspond, par exemple, à des grands

segments produits ou à des canaux de distribution. Elle permet de classifier les processus de l'entreprise, des unités organisationnelles ou des applications qui servent un produit spécifique et/ ou un marché spécifique. Les cadres réglementaires de certaines industries imposent leurs propres listes de lignes métier.

- Les processus métier qui utilisent l'application

  📖 *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.*

- Les capacités métier couvertes par l'application

  📖 *Une capacité métier est une unité de découpage des traitements d'un système d'information. Les traitements peuvent par exemple correspondre à une activité ou à un métier de l'entreprise.*

Responsabilités concernant une application

Propriétaire local d'application

Un propriétaire d'application est responsable de sa gestion tout au long du cycle de vie l'application. Il doit s'assurer que l'application est correctement décrite.

☛ *Le terme "propriétaire" identifie une personne ou une entité ayant accepté la responsabilité de la mise au point, de la maintenance, de l'utilisation des actifs. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur l'actif.*

Pour spécifier un ou plusieurs propriétaire(s) :

1. Dans la fenêtre de propriétés de l'application, dépliez la section **Responsabilités**.
2. Sélectionnez le sous-onglet **Propriétaire local d'application** et reliez un ou plusieurs utilisateurs.

Local IT Risk Manager

Le "Local IT Risk Manager" est le correspondant local du risque au niveau des applications.

☛ *Les applications qui sont reliées à un Local IT Risk Manager ou à un propriétaire local d'application apparaissent dans l'onglet de navigation **Accueil**, sous **Liste de tâches > Mes responsabilités > Mes actifs informatiques**.*

Technologies liées aux applications

A partir de la page de propriété d'une application, vous pouvez relier des technologies existantes ou en créer de nouvelles.

Pour accéder aux technologies depuis une application :

❱ Dans la fenêtre de propriétés d'une application, dépliez la section **Technologies**.

Données échangées

Ces informations sont issues de **HOPEX IT Portfolio Management**.

Les flux, leur orientation et leur contenu échangés entre les applications peuvent être décrits. Ces informations permettent de construire une cartographie des échanges.

> 🕮 *Un flux représente la circulation d'information à l'intérieur de l'entreprise ou entre l'entreprise et son environnement. Un flux peut transporter un contenu.*

Le contenu d'un flux est représenté par une donnée métier.

> 🕮 *Une donnée métier désigne le contenu d'un flux. Une donnée métier peut être utilisée par plusieurs flux puisqu'elle n'est pas associée à un émetteur et à un destinataire. Une même donnée métier peut être utilisée par plusieurs flux.*

Vulnérabilités d'une application

Pour consulter les vulnérabilités d'une application :

- Dans la fenêtre de propriétés de l'application, sélectionnez la page **Risques informatiques** puis dépliez la section **Vulnérabilités**.

Contrôles reliés à une application

Pour consulter les contrôles concernant une application :

- Dans la fenêtre de propriétés de l'application, sélectionnez la page **Contrôles**.

Décrire les technologies

> 🕮 *Une technologie est une définition ou un format qui a été approuvé par une organisation de standardisation ou qui est accepté comme standard de fait par l'industrie.*

Accéder aux technologies

Pour accéder à la liste de toutes les technologies :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Liste d'inventaires informatiques > Toutes les technologies**.

Définir les caractéristiques d'une technologie

Pour spécifier les caractéristiques techniques d'une technologie :

- Dans les pages des propriétés d'une application, cliquez sur la page **Caractéristiques** puis sur **Technologie**.

Vous pouvez renseigner le champ **Identification** de la technologie:

- le **Nom** de la technologie
- le **Code** interne
- le **Fournisseur**

Types de technologie

Vous pouvez spécifier le **Type de technologie** :

- services applicatifs
- système d'exploitation
- plateforme
- SGBD-R

Une technologie peut être reliée à un ou plusieurs types de technologie.

☛ *Seul l'administrateur fonctionnel peut créer de nouveaux types de technologie.*

Risques et vulnérabilités d'une technologie

Vous pouvez également relier la technologie à :

- des risques
- des vulnérabilités

🕮 *Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif.*

INVENTAIRE DES MENACES ET VULNÉRABILITÉS

Exemples de menaces, types de vulnérabilité et vulnérabilités

Types de vulnérabilité	Vulnérabilités	Menaces
Matériel	Sensible aux variations de températures	Evénement météorologique
Matériel	Stockage non sécurisé	Vol d'informations ou documents
Logiciel	Interface logicielle compliquée	Erreur d'utilisation
Réseau	Mot de passe non sécurisé	Accès non autorisé
Personnel	Absence de directives concernant l'utilisation des logiciels	Utilisation de logiciels non autorisés
Site	Emplacement du matériel dans une zone inondable	Inondation

Exemples tirés de la norme ISO 27005:2011

Consulter les menaces

Les menaces sont des facteurs externes ou internes qui mettent en danger les actifs informatiques de l'entreprise. Chaque menace regroupe un ensemble de vulnérabilités. Pour plus de détails, voir "Consulter les vulnérabilités", page 24.

Accéder aux menaces

Pour accéder aux menaces :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Inventaires > Menaces et vulnérabilités > Toutes les menaces**.

☛ *Vous pouvez également accéder aux menaces par type de menace. Voir "Caractéristiques des menaces", page 24.*

Créer un type de menace

Pour créer un type de menace :

1. A partir de l'inventaire, cliquez sur **Menaces et vulnérabilités > Menaces et vulnérabilités**.
2. Faites un clic droit sur la racine de l'arborescence "Menaces et vulnérabilités" et sélectionnez **Nouveau > Type de menace**.
   Le type de menace apparaît dans l'arborescence.

Caractéristiques des menaces

Vous pouvez :

- spécifier le type de menace à laquelle la menace appartient

  🕮 *Les types de menaces permettent de regrouper les menaces en différentes catégories (ex: dommage physique, évènements naturels, défaut technique, etc.). Pour en créer, voir "Créer un type de menace", page 24*

- relier des vulnérabilités à la menace dans la section correspondante.

  ☛ *Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif. Pour plus de détails, voir "Consulter les vulnérabilités", page 24.*

Consulter les vulnérabilités

Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif.

Elles peuvent être importées à partir de bases de données nationales ou d'outils de gestion des vulnérabilités.

Accéder aux vulnérabilités

Pour accéder aux vulnérabilités :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. A partir de la page des inventaires, cliquez sur **Menaces et vulnérabilités > Toutes les vulnérabilités**.

   ☛ *Vous pouvez également accéder aux vulnérabilités par type de vulnérabilité. Voir "Source", page 25.*

Créer un type de vulnérabilité

Pour créer un type de vulnérabilité:

1. A partir de la page des inventaires cliquez sur **Menaces et vulnérabilités > Vulnérabilités par type de vulnérabilité**.
2. Faites un clic droit sur la racine de l'arborescence "Vulnérabilités" et sélectionnez **Nouveau > Type de vulnérabilité**.
   Le type de vulnérabilité apparaît dans l'arborescence.

Caractéristiques des vulnérabilités

Menace

Il s'agit de la menace qui exploite potentiellement la vulnérabilité.

☛ *Une vulnérabilité ne peut relever que d'une seule menace.*

Type de vulnérabilité

Les types de vulnérabilité regroupent les vulnérabilités en différentes catégories (ex: Logicielle, Organisationnelle, Site (géographique), etc.).

☛ *Pour créer un type, voir "Créer un type de vulnérabilité", page 24.*

Date de publication initiale

La date de publication est la date à laquelle une vulnérabilité a été décrite pour la première fois.

Cette caractéristique est facultative. Elle peut être utile en cas d'import depuis une source tierce.

Dernière date de modification

La dernière date de modification est la date à laquelle la vulnérabilité a été modifiée.

Cette caractéristique est facultative. Elle peut être utile en cas d'import depuis une source tierce.

Source

Les vulnérabilités sont rendues disponibles et régulièrement mises à jour par des organismes nationaux ou de normalisation, par exemple :

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

Statut

- Potentiel
- Détecté
- Traité
- Fermé

Score de vulnérabilité

- Faible
- Moyen
- Élevé

Périmètre des vulnérabilités

Le périmètre des vulnérabilités se compose de deux sections :

- actifs
- actifs déployés

> ☛ *En pratique, l'un ou l'autre des liens sont utilisés, selon l'inventaire disponible (types ou déploiements)*
>
> ☛ *Voir "Positionner les vulnérabilités sur les actifs informatiques", page 36.*

Actifs informatiques vulnérables

- Applications

> 🕮 *Une application métier est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques et des fonctionnalités fournies aux utilisateurs.*

- Technologie logicielles

> 🕮 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

Actifs informatiques déployés vulnérables

- Installation logicielle

> 🕮 *Une installation logicielle représente le déploiement d'une application en vue de son utilisation sur un site donné.*

- Technologie déployée

> 🕮 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

Evaluation CVSS

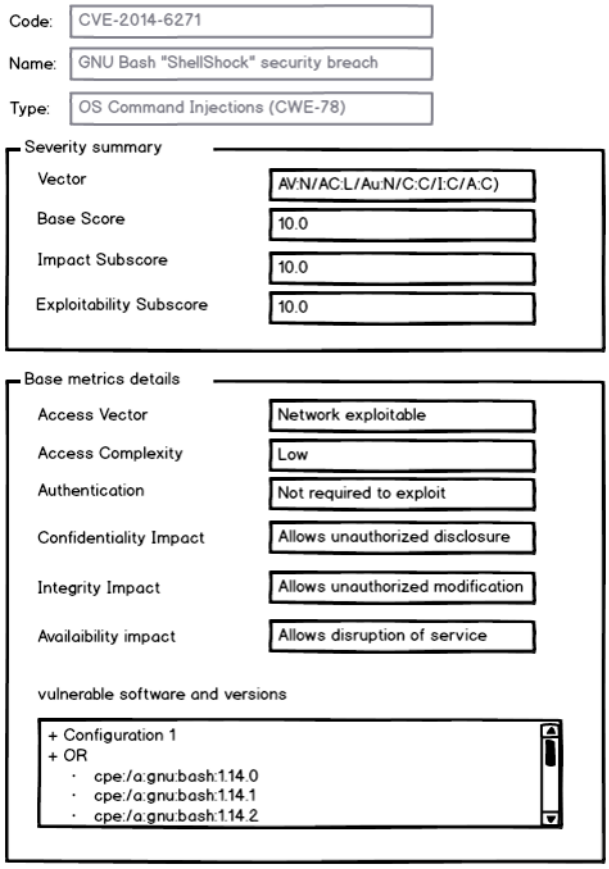
Common Vulnerability Scoring System est (CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.

CVSS est une notation édictée par le NIST (National Institue of Standards and Technology) aux USA et est un standard de fait.

> ☛ *Ces données sont à importer à partir d'outils tiers et ne sont pas saisies dans **HOPEX IT Risk Management**.*

Exemples de données

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



Rapports concernant les vulnérabilités

Divers rapports illustrent les vulnérabilités. Voir "Rapports concernant les vulnérabilités", page 94.

INVENTAIRE DES RISQUES ET CONTRÔLES

Consulter les risques

Accéder aux risques

Pour accéder aux risques :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Risques > Toutes les risques**.

Vous pouvez également accéder :

- aux risques clés

  ☛ *Les risques clés sont les risques pour lesquels la case Risque clé a été cochée dans la fenêtre de propriétés du risque.*

- aux risques non reliés à un contrôle

Caractéristiques évaluées

Impact

L'impact caractérise l'impact du risque lorsqu'il se manifeste.

Probabilité

La probabilité caractérise la probabilité que le risque se manifeste.

Risque inhérent

Le risque inhérent (ou brut) désigne le risque auquel l'organisation est exposée en l'absence de mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque. Il s'agit du produit de la valeur de l'impact par la valeur de la probabilité avant prise en compte des mesures de prévention ou d'atténuation du risque.

En résumé, risque inhérent = impact * probabilité

Vélocité

La vélocité représente la rapidité de propagation d'un risque depuis un actif sur les autres actifs si un incident survient. Elle représente un moyen de caractériser le risque (autrement que par l'impact et la fréquence).

Risque inhérent pondéré

Risque inhérent * vélocité

Périmètre du risque

Dans la fenêtre de propriétés d'un risque vous pouvez identifier :

- les actifs informatiques à risque
  - applications

    📖 *Une application métier est un ensemble de composants logiciels qui constituent un tout cohérent au regard des développements informatiques et des fonctionnalités fournies aux utilisateurs.*
  - technologies logicielles

    📖 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*
- les actifs déployés à risque
  - installations logicielles

    📖 *Une installation logicielle représente le déploiement d'une application en vue de son utilisation sur un site donné.*
  - technologies déployées

    📖 *Une technologie logicielle est un composant de base nécessaire au fonctionnement des applications métiers.*

Pour spécifier le périmètre du risque :

1. Dans la fenêtre de propriétés du risque, dépliez, selon le besoin, la section :
   - **Périmètre (actifs informatiques)**, ou
   - **Périmètre (actifs informatiques déployés)**

     ☛ *Le choix de la définition du périmètre du risque a un impact sur les évaluations directes.*
2. Reliez les objets qui vous conviennent.

   ☛ *Pour plus de détails sur le périmètre des risques, voir "Le périmètre d'un risque", page 510*

Analyse du risque

Pour plus de détails, voir "L'analyse d'un risque", page 510.

Evaluation du risque

L'évaluation des risques peut se faire par :

- application
- application déployée (ou installation)

  ☛ *L'onglet disponible dans la fenêtre de propriétés du risque est fonction du choix qui a été fait concernant l'évaluation des risques.*

Pour plus de détails, voir "Evaluer les risques à dire d'expert", page 42.

Traitement du risque

Pour plus de détails, voir "Spécifier les contrôles et actions à mettre en œuvre", page 75.

Consulter les contrôles

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

Il convient de noter qu'un contrôle mal implémenté peut représenter une vulnérabilité.

Accéder aux contrôles

Pour accéder aux contrôles :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Contrôles > Tous les contrôles**.

Vous pouvez relier des contrôles dans la fenêtre de propriétés d'un type de contrôle.

Périmètre d'un contrôle

Vous pouvez relier plusieurs types d'objets à un contrôle dans le cadre de **HOPEX IT Risk Management.**

Vous pouvez relier :

- les types d'objets présents dans le périmètre standard d'un contrôle : voir "Le périmètre d'un contrôle", page 514
- des applications (section **Périmètre (Actifs informatiques)**).

Evaluation de contrôles

L'onglet **Evaluation** de la fenêtre de propriétés d'un contrôle permet de faire une évaluation directe à partir du modèle d'évaluation "Evaluation des contrôles par applications".

Voir "Evaluer les contrôles à dire d'expert", page 46

Préparer l'environnement de travail pour les questionnaires

Avant de lancer une campagne d'évaluation vous devez avoir préparé l'environnement de travail. Assurez-vous d'avoir :

- relié des risques / contrôles aux applications

  ☛ *Pour plus de détails, voir "Identifier et positionner les risques", page 37.*

  ☛ *Dans l'optique d'obtenir des rapports pertinents, il peut être utile de relier les applications à des processus, lignes métier ou capacités métier. Ceci n'est toutefois pas nécessaire pour lancer des campagnes d'évaluation.*

- défini un propriétaire local d'application pour chaque application

  ☛ *Pour plus de détails, voir "Responsabilités concernant une application", page 20*

Pour plus de détails sur les évaluations, voir "Evaluations par questionnaires", page 51.

INVENTAIRE DES EXIGENCES ET RÉGLEMENTATIONS

Accéder aux exigences et réglementations

Pour accéder aux exigences et réglementations :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Réglementations et exigences**.
   Une arborescence de réglementations et exigences apparaît.

Caractéristiques des réglementations

> 🕮 *Une réglementation ou 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 de politiques internes.*

Pour plus de détails, voir "Caractéristiques d'une réglementation", page 516.

Dans la fenêtre de propriétés d'une réglementation vous pouvez relier :

- des processus métier (dans la section **Périmètre**)
- des sous-réglementations
- des exigences

Caractéristiques des exigences

> 🕮 *Une exigence est un besoin ou une attente formulé 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.*

Pour plus de détails, voir aussi "Caractéristiques des exigences", page 519.

Pour spécifier le paramètre d'une exigence :

❱ Dans la fenêtre de propriétés de l'exigence, sélectionnez la page **Périmètre**.
Dans la section **Eléments contributeurs**, vous pouvez renseigner :

- des **Types de contrôle**

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

- des **Contrôles**

INVENTAIRE DES FOURNISSEURS

📖 *Les fournisseurs informatiques peuvent être des éditeurs ou des prestataires de services.*

Accéder à la liste des fournisseurs

Pour accéder à la liste des fournisseurs :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Fournisseurs**.

Caractéristiques des fournisseurs

Type de fournisseur

Un fournisseur est une entité de type "Fournisseur".

Informations financières

Voir "Spécifier le coût des produits et services", page 48.

Informations de facturation

- Raison sociale
- Nom commercial fournisseur : nom d'usage, si différent de la raison sociale (en anglais : DBA, Doing Business As)
- Adresse de facturation fournisseur
- Téléphone

Informations concernant le contact principal

- Nom
- Adresse
- Email
- Titre : Poste occupé (par exemple Responsable de compte)

Liste des technologies fournies

Dans la fenêtre de propriétés du fournisseur vous pouvez consulter la liste des technologies qu'il fournit.

Evaluation de risque fournisseur

Dans cet onglet vous pouvez attribuer une note au fournisseur. Pour plus de détails, voir "Evaluer les fournisseurs", page 49.

Les questionnaires d'évaluation destinés à évaluer le fournisseur apparaissent également ici.

UTILISER HOPEX IT RISK MANAGEMENT

Une fois la bibliothèque des actifs informatiques constituée, **HOPEX IT Risk Management** vous permet de gérer les risques informatiques. La solution permet également de gérer la conformité informatique ainsi que les fournisseurs de technologies.

✓ "Gérer les risques informatiques", page 36
✓ "Gérer la conformité informatique", page 44
✓ "Gérer les fournisseurs informatiques", page 48

GÉRER LES RISQUES INFORMATIQUES

Après avoir dressé l'inventaire informatique de votre entreprise, vous pouvez :

- positionner les vulnérabilités sur les actifs informatiques
- identifier les risques
- positionner les risques sur les actifs informatiques
- identifier les scénarios de risque
- évaluer les risques à dire d'expert ou via des campagnes d'évaluation
- définir des plans d'action d'amélioration

Pour plus de détails sur les caractéristiques des risques, voir "Consulter les risques", page 28.

A tout moment vous pouvez produire des rapports concernant la gestion des risques informatiques, les menaces et vulnérabilités. Pour plus de détails, voir "Rapports concernant les risques informatiques", page 86.

Dresser l'inventaire informatique et identifier les vulnérabilités

Identifier les actifs informatiques

Pour pouvoir gérer les risques, les actifs doivent être clairement identifiés et un inventaire de tous les actifs doit être réalisé et géré.

☛ *Pour plus de détails, voir "Inventaire des actifs informatiques", page 18.*

Positionner les vulnérabilités sur les actifs informatiques

Vous pouvez identifier les vulnérabilités et les positionner sur les actifs (application ou technologie logicielle). Pour cela une matrice vous facilite la tâche.

☛ *Pour plus de détails sur les vulnérabilités, voir "Inventaire des menaces et vulnérabilités", page 23.*

Pour positionner les vulnérabilités sur les actifs :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Menaces et vulnérabilités > Contextualisation des actifs IT**.
3. Cliquez sur **Nouveau**.
4. Cliquez sur **Ajouter lignes** pour ajouter les vulnérabilités.
5. Cliquez sur **Ajouter colonnes** pour ajouter les actifs informatiques.

6. Cliquez dans les cellules qui vous intéressent pour relier vulnérabilités et actifs informatiques.

> ☛ *Pour accéder aux vulnérabilités des applications, voir "Vulnérabilités d'une application", page 21.*

Identifier et positionner les risques

Pour déduire les risques encourus par un actif informatique, vous pouvez :

- vous baser sur les vulnérabilités qui ont été identifiées dans la page de propriétés de cet actif.

> ☛ *Pour plus de détails, voir "Vulnérabilités d'une application", page 21.*

- vous baser sur les vulnérabilités reliées aux menaces.

> ☛ *Pour plus de détails, voir "Consulter les menaces", page 23.*

Une fois les risques identifiés, **HOPEX IT Risk Management** offre deux méthodes pour positionner les risques sur les actifs informatiques.

Positionner les risques via une matrice

Pour positionner les risques sur les actifs informatiques, vous pouvez utiliser une matrice spécifique.

Pour utiliser la matrice Risques x Actifs informatiques :

1. Cliquez sur **Bibliothèque > Risques > Matrice > Risques par actif informatique**.
2. Ajoutez :
   - des risques en ligne
   - des actifs informatiques en colonne
3. Cliquez dans les cellules qui vous intéressent pour relier vulnérabilités et actifs informatiques.

Positionner les risques individuellement sur chaque actif

Les risques peuvent être positionnés directement sur les actifs informatiques :

- applications
- technologies

En fonction de l'évaluation qui sera utilisée, vous pouvez choisir de positionner les risques sur :

- les applications
- les applications déployées

Pour plus de détails, voir "Périmètre du risque", page 29.

> ☛ *Veuillez noter que le choix du positionnement du risque a un impact dans le cadre de l'évaluation des risques. Deux modèles d'évaluation différents sont disponibles. Voir "Modèles d'évaluation des risques", page 43.*

Identifier les scénarios de risque

Si besoin, vous pouvez définir des scénarios de risques et identifier les relations de cause à effet entre les risques.

> 🕮 *Un scénario de risque informatique est la description d'un événement informatique, qui, s'il se produisait, pourrait avoir un impact sur l'activité de l'entreprise.*

Créer un scénario de risque

Pour créer un scénario de risque :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Risques > Scénarios de risque**.
3. Cliquez sur **Créer** puis sur **Suivant**.
4. Dans la section **Elements du scénario de risque**, reliez :
   - des applications, ou
   - des technologies logicielles

> ☛ *La section **Risques** ne présente pas les risques qui proviennent de l'initialisation du diagramme.*

Créer un diagramme de scénario de risque

Le IT RM Manager identifie des dépendances de type cause / conséquence entre risques depuis un diagramme de scénario de risques. Ce diagramme permet de créer un réseau de risques en vue d'identifier les risques pivots.

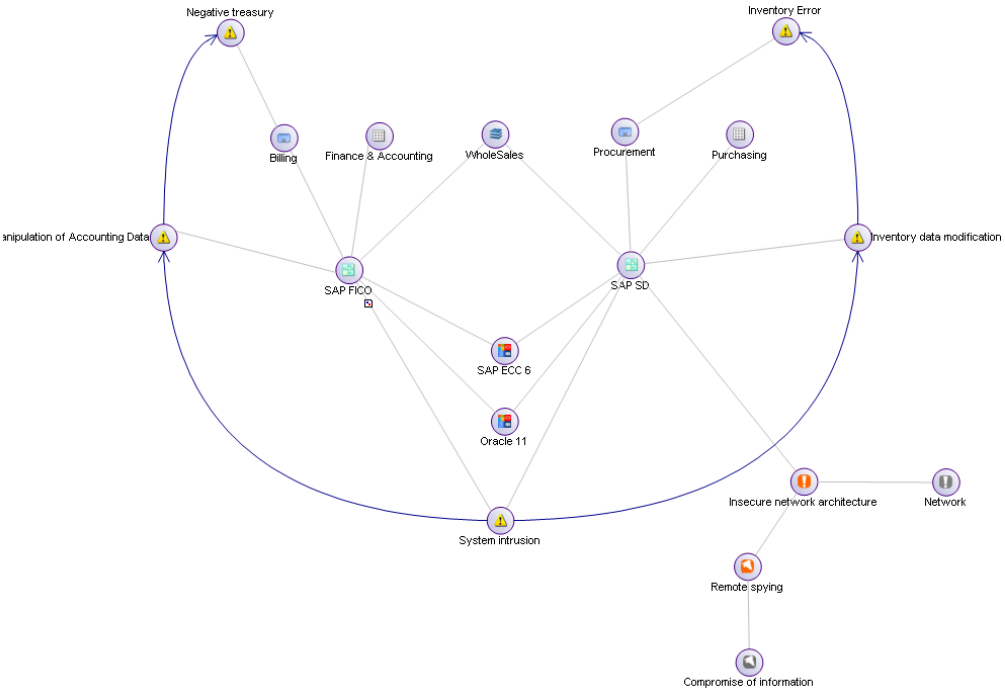
> ☛ *Pour plus de détails sur les risques pivots, voir "Risques pivots, causes et conséquences", page 39.*

Pour créer un diagramme de scénario de risque :

- Cliquez sur l'icône du scénario de risque et sélectionnez **Nouveau > Diagramme de scénario de risque**.

Les objets suivants sont positionnés automatiquement sur le diagramme :

- les applications ou technologies logicielles
- les vulnérabilités et menaces
- les processus, capacités métier et lignes métier reliés à l'application
- les risques associés



Exemple de diagramme de scénario de risque

Liens de causalité

Les risques sont reliés entre eux par des causalités (matérialisées par des liens). Ces liens de causalité sont spécifiques à un scénario.

Risques pivots, causes et conséquences

Les risques peuvent être considérés alternativement comme :

- cause
- conséquence
- risque pivot

Un risque pivot est un risque qui, dans un digramme de scénario de risques, est relié à au moins une cause et éventuellement une ou plusieurs conséquences.

☛ *Un même risque pivot peut avoir plusieurs causes et conséquences.*

Rapport de causalité de risques

Un rapport permet de récapituler les liens de causalité d'un diagramme de scénario de risque.

Pour accéder à ce rapport :

- Dans la fenêtre de propriétés d'un scénario de risque, sélectionnez la page **Rapport de causalités de risque**.

1. Risk Causuality

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

Exemple de causalités de risques

Ce rapport met en relief les "risques pivots" d'un scénario de risque, c'est-à-dire les risques se trouvant au milieu de la chaîne de risques.

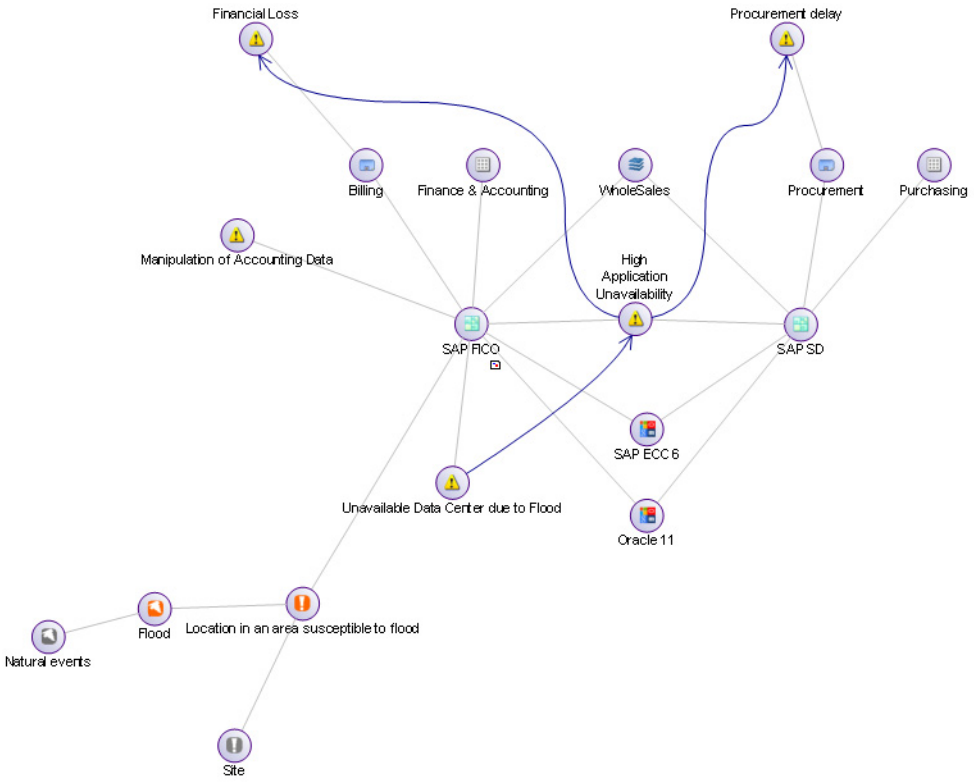
Cette chaîne de risques comporte :

- des risques apparemment mineurs comme causes (il peut par exemple s'agir de risques informatiques techniques par exemple)
- des risques potentiels majeurs comme conséquences (il peut par exemple s'agir de risques métier importants)

Le traitement des risques pivots constitue la clé permettant d'empêcher ces risques majeurs de survenir.

Exemples

Ci-dessous un diagramme de scénario illustré par le rapport de causalité qui lui correspond.



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

Evaluer les risques à dire d'expert

HOPEX IT Risk Management vous permet d'évaluer le niveau de risque à dire d'expert :

- par application, ou
- par application déployée (pour pouvoir évaluer les risques d'une entité)

> ☛ *Les risques peuvent être positionnés soit sur une application soit sur une application déployée. Pour plus de détails, voir "Périmètre du risque", page 29*

Evaluation directe des risques

L'évaluation à dire d'expert correspond à ce que nous appelons l'évaluation directe dans **HOPEX IT Risk Management** (c'est-à-dire sans définir une campagne d'évaluation par questionnaire).

Pour évaluer directement un risque :

1. Dans la fenêtre de propriétés d'un risque, sélectionnez l'une des pages dédiées aux évaluations :
   - **Evaluation par installation** : permet d'évaluer les risques par application déployée
   - **Evaluation par application**

   > ☛ *Une seule de ces pages apparaît, en fonction du choix que vous avez effectué concernant le positionnement des risques. Pour plus de détails, voir "Identifier et positionner les risques", page 37.*
2. Cliquez sur le bouton **Evaluation**.
3. Sélectionnez éventuellement un objet de contexte puis sélectionnez une valeur pour :
   - l'impact

     > 🕮 *L'impact caractérise l'impact du risque lorsqu'il se manifeste.*
   - la probabilité

     > 🕮 *La probabilité caractérise la probabilité que le risque se manifeste.*
   - la vélocité

     > 🕮 *La vélocité représente la rapidité de propagation d'un risque depuis un actif sur les autres actifs si un incident survient.*
4. Modifiez éventuellement la **Date de mesure** et cliquez sur **OK**.

Modèles d'évaluation des risques

Modèle d'évaluation	Objet évalué	Contexte	Mode	Caractéristiques évaluées	Évaluateur
Évaluation des risques par application	Risque relié à application	Application reliée au risque	direct ou par campagne	- Impact - Probabilité - Risque Inhérent - Vélocité - Risque inhérent pondéré	- Évaluation directe : IT RM Manager - Par campagne : Propriétaire d'application
Évaluation des risques par application déployée	Risque relié à chaque application déployée	Application déployée	direct ou par campagne	- Impact - Probabilité - Risque Inhérent - Vélocité - Risque inhérent pondéré	- Évaluation directe : IT RM Manager - Par campagne : Propriétaire d'application

☛ *Ces modèles d'évaluation peuvent également être utilisés dans le cadre des campagnes d'évaluation. Pour plus de détails, voir "Evaluations par questionnaires", page 51.*

Définir les plans d'action d'amélioration

Le IT RM Manager :

- définit les plans d'action de maîtrise informatique en tant que propriétaire de plan d'action
- assigne les actions aux propriétaires d'application responsables de leur mise en œuvre.

☛ *Vous pouvez relier des plans d'action à des actifs informatiques.*

Pour plus de détails sur les plans d'action, voir "Traiter les risques", page 73.

GÉRER LA CONFORMITÉ INFORMATIQUE

Dans le cadre de la gestion des risques informatiques, les contrôles sont utilisés dans une optique de conformité.

Vous pouvez :

- documenter les contrôles relatifs aux applications gérées dans le cadre des cadres réglementaires en vigueur (ex : ISO 2700x).
- relier ces contrôles aux exigences réglementaires à respecter.

☛ *Pour plus de détails sur les contrôles, voir "Les contrôles", page 513.*

- évaluer les contrôles à dire d'expert ou via des campagnes d'évaluation.

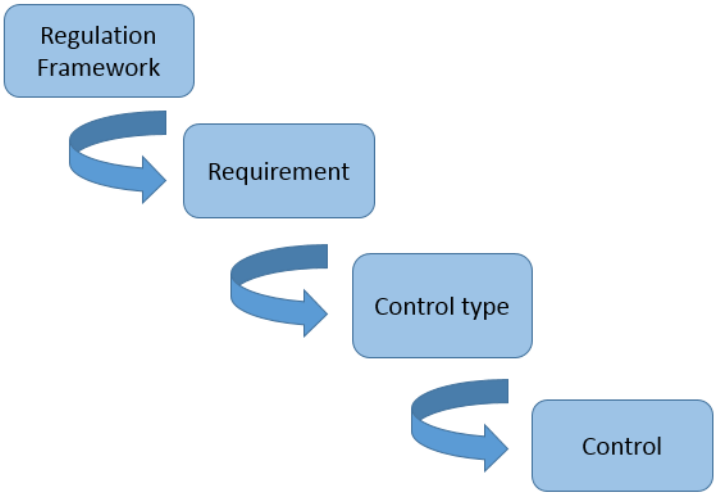
A tout moment, vous pouvez produit des rapports de synthèse de la conformité aux cadres réglementaires en vigueur et de l'efficacité du dispositif de contrôle.

☛ *Pour plus de détails, voir "Rapports concernant la conformité informatique", page 97.*

Dresser l'inventaire des contrôles et types de contrôles

Liens entre Contrôles et Contrôles types

Si vous souhaitez relier un contrôle à une exigence vous devez en fait lui relier le type de contrôle correspondant.



Relier les types de contrôles aux exigences réglementaires

Pour relier les contrôles aux exigences à respecter :

1. Dans la fenêtre de propriétés d'une exigence, sélectionnez la page **Périmètre** et dépliez la section **Eléments contributeurs**.
2. Reliez un ou plusieurs contrôles.

Définir le périmètre applicatif du contrôle

Pour définir les applications concernées par un contrôle :

1. Dans la fenêtre de propriétés d'une application, sélectionnez la page **Contrôles** et créez un contrôle.
2. Dans la fenêtre de propriétés du contrôle ainsi créé, dépliez la section **Périmètre** et reliez un **Type de contrôle**.

Définir les exigences réglementaires à respecter

Le IT RM Manager définit les exigences réglementaires à respecter pour les différents cadres réglementaires en vigueur.

☛ *Les réglementations, exigences ou types de contrôle peuvent être importés depuis un inventaire compatible UCF (Unified Compliance Framework®, par exemple).*

Pour accéder aux exigences :

- Dans la page des inventaires, cliquez sur **Réglementations et exigences.**

☛ *Pour plus de détails sur les réglementations et exigences, voir "L'environnement réglementaire", page 516.*

Identifier les contrôles sur les applications

Le IT RM Manager identifie, pour chaque application dont il a la charge :

- les cadres réglementaires ou exigences qui s'appliquent
- les contrôles, sur la base de l'inventaire de contrôles prédéfini ou créés spécifiquement

Pour définir les contrôles sur une application :

1. Dans la fenêtre de propriétés de l'application, sélectionnez la page **Contrôles**.
2. Créez ou reliez les contrôles applicables.

> ☛ *Il est nécessaire de relier les contrôles aux applications pour pouvoir procéder à des évaluations.*

Evaluer les contrôles à dire d'expert

Le IT RM Manager peut évaluer directement les contrôles et ainsi en déduire la conformité aux réglementations. Il s'agit d'une évaluation à dire d'expert.

Evaluer directement les contrôles

Pour évaluer directement les contrôles déployés sur les applications :

1. Dans la fenêtre de propriétés d'un contrôle, sélectionnez la page **Evaluation des contrôles**.
2. Cliquez sur le bouton **Evaluer**.
   La liste des applications concernées par ce contrôle vous est proposée.
3. Qualifiez la **Conception** du contrôle
   - Adéquat
   - Inadéquat
4. Qualifiez l'**Efficacité** du contrôle.
   - Efficace
   - Inefficace
5. Modifiez éventuellement la **Date de mesure** et cliquez sur **OK**.

> ☛ *La date de la mesure est par défaut la date du jour. Vous pouvez sélectionner une date antérieure à la date du jour.*

Le **Niveau de contrôle** est automatiquement calculé à partir des valeurs des caractéristiques renseignées.

> 🕮 *Le niveau de contrôle caractérise le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour évaluer le risque.*
>
> ☛ *Le niveau de contrôle est jugé "Satisfaisant" si le contrôle est jugé à la fois :*
>
> - *efficace*
> - *adéquat*

Modèle utilisé pour l'évaluation des contrôles

Modèle d'évaluation	Objet évalué	Contexte	Mode	Caractéristiques évaluées	Évaluateur
Évaluation des contrôles par application	Contrôle	Application reliée au contrôle	direct ou par campagne	- Conception - Efficacité	- IT RM Manager (direct) - Propriétaires de contrôles (campagnes)

☛ *Ce modèle d'évaluation est également utilisé lors de l'évaluation des contrôles via des campagnes.*

GÉRER LES FOURNISSEURS INFORMATIQUES

HOPEX IT Risk Management vous permet d'identifier les fournisseurs informatiques (éditeurs de logiciels ou prestataires).

Vous pouvez :

- spécifier le coût des produits et services achetés auprès de chaque fournisseur pour l'année écoulée.
- évaluer les fournisseurs en leur attribuant une valeur, en vous basant éventuellement sur les questionnaires envoyés via des campagnes.

Vous pouvez à tout moment produire des rapports de synthèse concernant le score des fournisseurs. Pour plus de détails, voir "Rapports concernant la gestion des fournisseurs", page 105.

Identifier les fournisseurs informatiques

L'administrateur fonctionnel IT RM identifie les fournisseurs informatiques (éditeurs, prestataires).

☛ *Pour plus de détails sur les fournisseurs, voir "Inventaire des fournisseurs", page 33.*

☛ *Les fournisseurs et technologies peuvent avoir été identifiés au préalable dans **HOPEX IT Portfolio Management** ou **HOPEX IT Architecture**.*

Spécifier le coût des produits et services

Chaque année, le IT RM Manager saisit un élément de coût global annuel des produits ou services achetés auprès du fournisseur.

Sur cette base il détermine le rang du fournisseur.

☛ *Ces informations sont saisies à titre documentaire dans **HOPEX IT Risk Management**.*

Pour saisir ces coûts :

1. Voir "Accéder à l'inventaire informatique", page 19
2. Cliquez sur **Fournisseurs**.
3. Sélectionnez un éditeur dans la liste qui vous est proposée.
4. Dans la fenêtre de propriétés de l'éditeur, sélectionnez la page **Information Fournisseur**.

5. Dans la fenêtre de propriétés, renseignez les données de la section **Informations financières** :
   - Montant total des achats
   - Rang

   ☛ *Les données de cette section correspondent aux données de la fin de l'année qui précède l'année en cours.*

Vous pouvez également renseigner les données suivantes :

- Coordonnées
- Informations de facturation

☛ *Pour plus de détails, voir "Inventaire des fournisseurs", page 33.*

Evaluer les fournisseurs

Le IT RM Manager peut évaluer le risque lié à un fournisseur.

Pour évaluer un fournisseur :

1. Voir "Accéder à l'inventaire informatique", page 19.
2. Cliquez sur **Fournisseurs**.
3. Sélectionnez un fournisseur dans la liste qui vous est proposée.
4. Dans la fenêtre de propriétés, sélectionnez la page **Risque fournisseur**.
5. Saisissez une valeur de manière à caractériser le risque lié au fournisseur.

   ☛ *Vous pouvez également lancer des campagnes dans le but d'évaluer le fournisseur et confirmer éventuellement votre estimation Dans ce cas l'évaluateur est à définir dans la session d'évaluation. Pour plus de détails, voir "Evaluations par questionnaires", page 51.*

EVALUATIONS PAR QUESTIONNAIRES

HOPEX permet de réaliser des évaluations à partir de questionnaires standards. Les questionnaires d'évaluation sont envoyés aux destinataires appropriés.

Le présent chapitre décrit le principe des évaluations par questionnaires.

☛ *Les solutions **HOPEX** permettent de procéder à des évaluations :*

- *à dire d'expert (appelées évaluations directes)*
- *via des campagnes d'évaluation permettant l'envoi de questionnaires, qui est abordé ici.*

✓ "Principe de l'évaluation par campagnes", page 52
✓ "Créer une campagne d'évaluation", page 54
✓ "Créer une session d'évaluation", page 55
✓ "Planifier les sessions au sein de la campagne (facultatif)", page 57
✓ "Valider la campagne d'évaluation", page 60
✓ "Visualiser les objets à évaluer et leurs contextes", page 61
✓ "Définir le périmètre de la session et les répondants", page 62
✓ "Valider les objets à évaluer et leur contexte", page 63
✓ "Envoyer les questionnaires", page 65
✓ "Remplir les questionnaires", page 66
✓ "Suivre l'avancement des questionnaires", page 68
✓ "Fermer la session d'évaluation", page 71

PRINCIPE DE L'ÉVALUATION PAR CAMPAGNES

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

Présentation des concepts

Session d'évaluation

📖 *Une session d'évaluation est une évaluation lancée sur un laps de temps déterminé. Le démarrage de la session d'évaluation a pour effet d'envoyer un questionnaire aux utilisateurs ciblés.*

Questionnaire

Des questionnaires d'évaluation sont envoyés aux **répondants** appropriés.

📖 *Un questionnaire propose une liste de questions prédéfinies qui peuvent être appliquées à un contrôle.*

Campagne d'évaluation

Avec les solutions **HOPEX**, une session d'évaluation est lancée dans le cadre d'une campagne d'évaluation.

📖 *Une campagne permet de regrouper plusieurs sessions.*

Etapes de l'évaluation

Préparer l'environnement de travail

Avant de lancer une campagne d'évaluation vous devez avoir préparé l'environnement de travail.

☛ *Pour plus de détails, voir "Préparer l'environnement de travail pour les questionnaires", page 30.*

Lancer une campagne et ses sessions d'évaluation

Voir "Etapes indicatives du workflow d'évaluation avec campagne", page 45:

> ☛ *Pour connaître toutes les possibilités offertes par **HOPEX**, voir "Workflows liés aux évaluations", page 150.*

- ✓ "Créer une campagne d'évaluation", page 54
- ✓ "Créer une session d'évaluation", page 55
- ✓ "Planifier les sessions au sein de la campagne (facultatif)", page 57

> ☛ *La planification de la campagne est une étape facultative. Si vous ne déployez pas la campagne d'évaluation, voir directement "Valider la campagne d'évaluation", page 60.*

- ✓ "Valider la campagne d'évaluation", page 60
- ✓ "Visualiser les objets à évaluer et leurs contextes", page 61
- ✓ "Définir le périmètre de la session et les répondants", page 62
- ✓ "Valider les objets à évaluer et leur contexte", page 63
- ✓ "Envoyer les questionnaires", page 65

> ☛ *Les étapes de déploiement, validation et démarrage de session ne sont pas à effectuer si vous décidez de lancer immédiatement la session après sa création ou si vous la planifiez dans l'assistant de création. Voir "Variantes de lancement d'une session d'évaluation", page 21.*

Une fois que les sessions d'évaluation sont lancées, vous pouvez :

- ✓ "Remplir les questionnaires", page 66
- ✓ "Suivre l'avancement des questionnaires", page 68
- ✓ "Fermer la session d'évaluation", page 71

CRÉER UNE CAMPAGNE D'ÉVALUATION

📖 *Une campagne permet de regrouper plusieurs sessions.*

Vous pouvez créer une campagne d'évaluation :

- ***A partir d'un modèle***
  La création d'une campagne à partir d'un modèle permet :
  - de réutiliser le même modèle sur toutes les sessions d'évaluation
  - de définir et de planifier le périmètre des sessions en répartissant les éléments à évaluer au sein de différentes sessions
- ***Sans modèle***
  Dans le cas de la création d'une campagne sans modèle, un modèle peut être indiqué au moment de la création de chaque session.

  ☛ *Cette rubrique présente la création d'une campagne d'évaluation avec un modèle d'évaluation livré en standard. Les possibilités offertes par les campagnes d'évaluation sans modèle sont décrites dans le guide **HOPEX Assessment**.*

Accéder aux campagnes d'évaluation

Pour accéder aux campagnes d'évaluation :

❱ Depuis le menu de navigation principal, cliquez sur **Gestion des campagnes > Campagnes.**

Créer une campagne d'évaluation

Pour créer une *campagne* d'évaluation :

1. Sélectionnez **Gestion des campagnes > Campagnes > Campagnes > Campagnes**.
   La liste des campagnes apparaît dans la zone d'édition.
2. Cliquez sur **Nouveau**.
   La page de création d'une campagne apparaît.
3. Dans le champ **Type de campagne**, sélectionnez "Avec modèle".
4. Sélectionnez le **Modèle d'évaluation** souhaité.
5. Modifiez éventuellement le **Calendrier**.

   ☛ *Le calendrier sert à initialiser les dates de début et de fin de la campagne d'évaluation.*
6. Renseignez la **Date de Début** et la **Date de fin** de l'évaluation.
7. Cliquez sur **Suivant** puis sur **OK**.
   La campagne est créée.

Avec les modèles d'évaluation fournis en standard dans la solution **HOPEX IT Risk Management**, vous devez préciser les objets à évaluer sur une session d'évaluation.

Voir "Créer une session d'évaluation", page 55.

CRÉER UNE SESSION D'ÉVALUATION

📖 *Une session d'évaluation est une évaluation lancée sur un laps de temps déterminé. Le démarrage de la session d'évaluation a pour effet d'envoyer un questionnaire aux utilisateurs ciblés.*

Accéder aux sessions d'évaluation

Pour accéder à une session d'évaluation :

1. Cliquez sur **Campagnes d'évaluation** et sélectionnez la campagne d'évaluation qui vous intéresse.

   ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

2. Dans la fenêtre de propriétés de la campagne d'évaluation, sélectionnez la page **Sessions**.

Créer une session d'évaluation

Créer une session d'évaluation

Pour créer une session d'évaluation :

1. Dans la fenêtre de propriétés de la campagne, cliquez sur la page **Sessions**.
2. Dans le cadre **Sessions d'évaluation**, cliquez sur **Nouveau**.
   Vous pouvez choisir de démarrer la session d'évaluation plus tard sans préciser quand.
3. Pour cela, dans la fenêtre de démarrage de la session, choisissez l'option "**pas maintenant**"

   ☛ *Cette option vous permet de compléter les données de la session d'évaluation, par exemple le responsable de la session et les dates de l'évaluation. Dans le cadre d'une campagne d'évaluation avec modèle, le modèle de session est renseigné par défaut. Il ne peut être modifié. Pour plus de détails sur la création de sessions d'évaluation sans modèle (mode ad-hoc ou avancé), voir "Créer une session d'évaluation Ad-hoc", page 25 ou "Créer une session d'évaluation avancée", page 27.*

   ☛ *Vous pouvez également choisir de démarrer la session d'évaluation maintenant ou de la planifier. Voir "Créer et lancer une session d'évaluation", page 56.*

4. Cliquez sur le bouton **Enregistrer**.
5. Créez éventuellement et de la même manière d'autres sessions d'évaluation.

   ☛ *Les sessions d'évaluation créées vont être utilisées pour planifier la campagne d'évaluation, c'est-à-dire répartir entre les différentes sessions d'évaluation les objets à évaluer dans leur contexte. Voir "Répartir les évaluations au sein des différentes sessions", page 58.*

Prévisualiser les paramètres de la session d'évaluation

Une fois la session d'évaluation créée, vous pouvez prévisualiser les paramètres hérités de la campagne d'évaluation.

> ☛ *Pour accéder à une session d'évaluation, voir "Accéder aux sessions d'évaluation", page 55.*

Pour prévisualiser les paramètres :

1. Ouvrez la fenêtre de propriétés de la session d'évaluation et cliquez sur l'onglet **Paramètres et prévisualisation**.
   Les éléments qui vont être évalués apparaissent.
   Vous pouvez visualiser notamment :
   - les caractéristiques évaluées (définies dans le modèle d'évaluation)

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

     > 🕮 *Un objet de contexte est un objet dans le cadre duquel l'évaluation est effectuée. Par exemple, un risque peut être évalué dans le cadre d'une application ou d'une application déployée.*
   - les nœuds d'évaluation, qui correspondent aux objets placés dans les différents objets contextes, associés aux répondants.

     > 🕮 *Un nœud d'évaluation est associé aux valeurs calculées depuis les réponses fournies dans le questionnaire par le répondant pour chacune des caractéristiques évaluées. Il est créé soit au moment du déploiement de la session d'évaluation soit au moment de l'agrégation. Les objets créés lors du déploiement sont détenus par la session et permettent de déterminer l'objet qui sera évalué, par qui et dans quel contexte.*

Créer et lancer une session d'évaluation

Voir "Créer une session d'évaluation", page 55.

Vous pouvez créer une session d'évaluation et choisir de la lancer :

- "**maintenant**"
  Si vous choisissez cette option, le lancement de le session sera effectuée sous vos yeux. Cette option permet de factoriser et d'exécuter en même temps les transitions de workflow suivantes :
  - déployer : "Visualiser les objets à évaluer et leurs contextes", page 61
  - valider : "Valider les objets à évaluer et leur contexte", page 63
  - démarrer : "Envoyer les questionnaires", page 65
- après sauvegarde des mises à jour, en mode batch ("**au plus tôt**")
- plus tard, en précisant la date et l'heure au format UTC ("**planifié**")

PLANIFIER LES SESSIONS AU SEIN DE LA CAMPAGNE (FACULTATIF)

Cette étape facultative est utile lorsque vous créez plusieurs sessions d'évaluation.

En effet vous pouvez passer directement :

- de l'étape "Créer une session d'évaluation", page 55:
- à l'étape "Valider la campagne d'évaluation", page 60

Vous pouvez choisir de planifier les sessions d'évaluation au sein de la campagne. Si c'est le cas, vous devez suivre les sous-étapes suivantes :

- déployer la campagne d'évaluation
- définir le périmètre de la campagne d'évaluation
- répartir les évaluations au sein des différentes sessions

Déployer une campagne d'évaluation

Le déploiement d'une campagne d'évaluation consiste à indiquer à l'avance les objets à évaluer au niveau de chaque session de la campagne.

> ☛ *Cette étape est facultative. Si vous ne souhaitez pas déployer la campagne d'évaluation, voir directement "Valider la campagne d'évaluation", page 60*

Pour déployer une campagne :

1. Dans la liste des campagnes, cliquez sur l'icône de la campagne que vous avez créée et sélectionnez **Campagne d'évaluation (En préparation) > Déployer**.

   > ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

2. Dans la fenêtre de déploiement, indiquez que vous souhaitez déployer la campagne immédiatement.

   > ☛ *Une fenêtre vous demande si vous souhaitez déployer la campagne:*
   >
   > - *maintenant*
   > - *dès que possible (après publication)*
   > - *à une date ultérieure*

3. Cliquez sur **OK**.
   Des nœuds d'évaluation sont créés.

   > 🕮 *Un nœud d'évaluation est constitué de :*
   >
   > - *un objet à évaluer*
   > - *un répondant (ou une assignation, c'est-à-dire un répondant associé à un rôle métier particulier)*
   > - *éventuellement, un ou plusieurs objets contextes (entités et processus)*

Vous pouvez maintenant définir le périmètre de la campagne d'évaluation. Voir "Définir le périmètre de la campagne d'évaluation et les répondants", page 58.

Définir le périmètre de la campagne d'évaluation et les répondants

Après avoir déployé la campagne d'évaluation, vous devez :

- définir son périmètre, c'est-à-dire sélectionner les nœuds d'évaluation que vous souhaitez inclure.
- spécifier les répondants.

☛ *Pour plus de détails sur les nœuds d'évaluation, voir "Déployer une campagne d'évaluation", page 57.*

Définir le périmètre de la campagne d'évaluation

Pour définir le périmètre de la campagne :

1. Dans la fenêtre de propriétés de la campagne, sélectionnez l'onglet **Périmètre effectif**.

   ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

   La liste des nœuds d'évaluation issus de votre déploiement apparaît.
2. Sélectionnez les valeurs que vous souhaitez retirer de la campagne et cliquez sur le bouton **Invalider**.

Spécifier les répondants

Pour ajouter ou modifier des répondants :

- Sélectionnez les éléments qui vous intéressent et cliquez sur **Définir un répondant**.

Répartir les évaluations au sein des différentes sessions

Une fois le périmètre de la campagne défini et les sessions d'évaluation créées, vous pouvez planifier la campagne.

Il s'agit de répartir les évaluations au sein des différentes sessions d'évaluation.

Pour planifier la campagne :

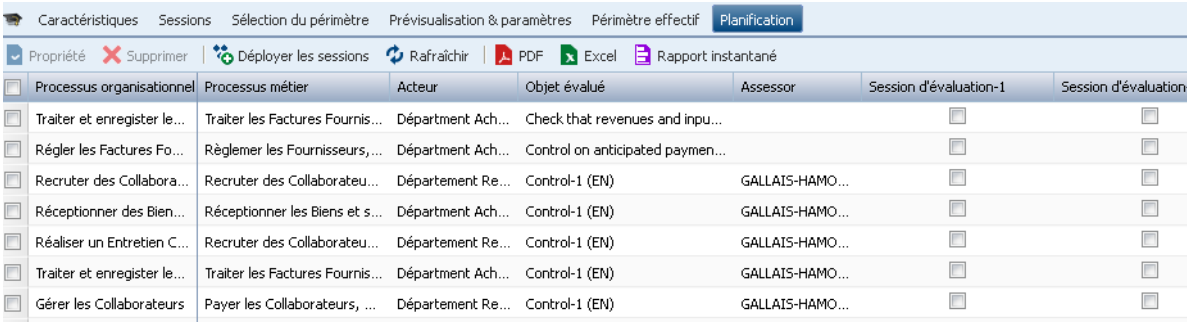
1. Dans la fenêtre de propriétés de la campagne d'évaluation, cliquez sur l'onglet **Planification**.

   ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

   L'onglet **Planification** n'est visible que lorsque des sessions d'évaluation ont été créées.

2. Dans la partie droite de la fenêtre, sélectionnez les sessions d'évaluation dans lesquelles vous souhaitez évaluer tel objet dans son contexte.

   ☛ *Si vous ne voyez pas apparaître les sessions d'évaluation que vous avez créées préalablement, cliquez sur le bouton* ***Rafraîchir****.*



☛ *Les répondants sont spécifiés à l'étape "Définir le périmètre de la campagne d'évaluation et les répondants", page 58.*

VALIDER LA CAMPAGNE D'ÉVALUATION

Vous pouvez valider la campagne d'évaluation :

- directement après avoir créé une session, ou
- après avoir planifié la campagne

> ☛ *Pour plus de détails, voir "Créer une session d'évaluation", page 55 et "Planifier les sessions au sein de la campagne (facultatif)", page 57*

La validation de la campagne d'évaluation a pour effet de figer ses paramètres (par exemple le périmètre ou la planification).

Pour valider la campagne :

1. Cliquez sur l'icône de la campagne et sélectionnez **Campagne d'évaluation (En préparation) > Valider**.

> ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

Vous pouvez maintenant préparer le lancement de la session d'évaluation et déployer la session d'évaluation. Voir "Visualiser les objets à évaluer et leurs contextes", page 61.

VISUALISER LES OBJETS À ÉVALUER ET LEURS CONTEXTES

Après avoir validé votre campagne, vous devez définir les objets à évaluer et leurs contextes. Pour cela vous devez ***déployer la session d'évaluation***.

Déployer permet de calculer l'ensemble des nœuds d'évaluation possibles pour la session.

> 🕮 *Un nœud d'évaluation est constitué de :*
>
> - *un objet à évaluer*
> - *un répondant (ou une assignation, c'est-à-dire un répondant associé à un rôle métier particulier)*
> - *éventuellement, un ou plusieurs objets contextes (entités et processus)*

Le responsable de la session peut ensuite revoir cette liste.

Pour créer la liste des nœuds d'évaluation d'une session :

1. Ouvrez la fenêtre de propriétés de la campagne et sélectionnez l'onglet **Session**.

   > ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

2. Dans la section **Session d'évaluation**, faites un clic sur la session qui vous intéresse et sélectionnez **Session d'évaluation (A soumettre) > Déployer**.

   > ☛ *Une fenêtre intermédiaire vous demande si vous souhaitez exécuter le déploiement maintenant, dès que possible (après publication) ou à une date planifiée.*

   Cette opération peut prendre quelques minutes.

DÉFINIR LE PÉRIMÈTRE DE LA SESSION ET LES RÉPONDANTS

Après avoir déployé la session d'évaluation, vous pouvez :

- sélectionner les nœuds d'évaluation que vous souhaitez inclure dans votre session, c'est-à-dire définir le périmètre de la session.
- spécifier les répondants.

> ☛ *Si vous avez défini le périmètre sur la campagne d'évaluation, vous n'avez pas forcément besoin de le redéfinir sur la session d'évaluation. Pour plus de détails, voir "Définir le périmètre de la campagne d'évaluation et les répondants", page 58.*

Définir le périmètre de la session

Pour accéder à la liste des nœuds d'évaluation calculés :

❱ Ouvrez la fenêtre de propriétés de la session d'évaluation et sélectionnez l'onglet **Paramètre effectif**.

> ☛ *Pour accéder à la session, voir "Accéder aux sessions d'évaluation", page 55.*

Vous pouvez maintenant sélectionner les objets à évaluer dans la session.

A partir de cette liste vous pouvez :

- dupliquer, valider, invalider ou supprimer des éléments à évaluer
- leur affecter un répondant.

Spécifier les répondants

Pour ajouter ou modifier des répondants :

❱ Dans l'onglet **Périmètre effectif** de la fenêtre de propriétés de la session, sélectionnez les éléments qui vous intéressent et cliquez sur **Définir un répondant**.

> ☛ *Pour accéder à la session, voir "Accéder aux sessions d'évaluation", page 55.*

VALIDER LES OBJETS À ÉVALUER ET LEUR CONTEXTE

La validation de la session d'évaluation permet de valider les objets à évaluer dans leur contexte ainsi que les répondants.

Cette validation a pour effet de ***générer les questionnaires*** sans toutefois les envoyer aux destinataires.

Valider la session d'évaluation

Pour valider la session et par conséquent générer les questionnaires :

1. Ouvrez la fenêtre de propriétés de la campagne et sélectionnez l'onglet **Session**.

   ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

2. Dans la section **Session d'évaluation**, cliquez sur la session qui vous intéresse puis sur **Session d'évaluation > Valider**.
   Tous les questionnaires sont créés avec le statut "A envoyer". Cette opération peut prendre quelques minutes.

Vous pouvez maintenant visualiser les questionnaires qui ont été générés.

Visualiser les questionnaires générés

Pour visualiser les questionnaires générés :

1. Dans la fenêtre de propriétés d'une session d'évaluation, sélectionnez l'onglet **Questionnaires.**

   ☛ *Pour accéder à la session, voir "Accéder aux sessions d'évaluation", page 55.*

2. Sélectionnez la ligne correspondant à la session d'évaluation et cliquez sur **Afficher les questionnaires**.
3. Ouvrez chacun des questionnaires pour afficher les nœuds d'évaluation et les questions associées à chacun d'entre eux.

   ☛ *Si la présentation des questionnaires ne vous convient pas, l'administrateur fonctionnel peut encore la modifier à ce stade. Pour plus de détails, voir le guide **HOPEX Assessment**, chapitre "Les modèles d'évaluation". Dans la solution, les modèles de questionnaires sont disponibles dans l'onglet concernant la gestion des campagnes **> Préparation > Modèles de questionnaire**.*

   ☛ *A ce stade vous pouvez encore modifier la présentation des questionnaires.*

   ☛ *Il est recommandé de valider la session d'évaluation juste avant de démarrer la session. En effet, si vous la validez trop tôt, les informations concernant les répondants risquent d'être erronées.*

Re-générer les questionnaires

Vous pouvez avoir besoin de re-générer les questionnaires si par exemple vous décidez de modifier les répondants avant de démarrer la session d'évaluation.

Pour re-générer les questionnaires :

- Faites un clic droit sur la session d'évaluation concernée et sélectionnez **Session d'évaluation (A démarrer) > Re-générer les questionnaires**.

  ☛ *Pour accéder à la session, voir "Accéder aux sessions d'évaluation", page 55.*

ENVOYER LES QUESTIONNAIRES

Après avoir validé la session d'évaluation, vous pouvez ***démarrer la session d'évaluation***, ce qui a pour effet d'envoyer les questionnaires aux répondants.

Pour démarrer la session d'évaluation :

1. Sélectionnez **Campagnes d'évaluation > Campagnes > Campagnes**.
   La liste des campagnes apparaît dans l'arbre de navigation.
2. Sélectionnez la campagne qui vous intéresse et cliquez sur **Propriétés**.
   La fenêtre de propriétés de la campagne apparaît dans la zone d'édition.
3. Dans l'onglet **Sessions**, cliquez sur la session qui vous intéresse puis sur **Session d'évaluation > Démarrer**.
   La page d'activation de la session apparaît.
4. Cliquez sur le bouton **Enregistrer** en haut de la page.
   Les *questionnaires d'évaluation* sont envoyés aux répondants définis dans le périmètre de la session d'évaluation.

REMPLIR LES QUESTIONNAIRES

Les étapes décrites ici concernent les répondants aux questionnaires.

☛ *Pour plus de détails sur les étapes du traitement d'un questionnaire, voir l'annexe au paragraphe concernant le workflow des questionnaires.*

Accéder aux questionnaires d'évaluation

Suite au lancement d'une session d'évaluation, les destinataires d'un questionnaire reçoivent une notification.

Pour répondre aux questionnaires :

1. Cliquez sur **Accueil > Mon bureau > Questionnaires > Mes questionnaires d'évaluation**.
   La liste des questionnaires à remplir apparaît.
2. Sélectionnez le questionnaire qui vous intéresse et cliquez sur **Afficher le questionnaire**.
3. Sélectionnez tour à tous les questions et répondez-y dans la partie inférieure de la fenêtre.
4. Cliquez sur **Enregistrer**.
5. Fermez la fenêtre d'affichage du questionnaire.
6. Cliquez sur le questionnaire dans la liste des questionnaires et sélectionnez **Questionnaire d'évaluation (A remplir) > Soumettre les réponses**.

   ☛ *Les questionnaires sont visibles à partir de ce menu tant que la session d'évaluation n'est pas fermée. Si la session d'évaluation est fermée, vous pouvez les consulter dans l'onglet **Questionnaires** de la fenêtre de propriétés de celle-ci.*

Demander le transfert d'un questionnaire

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

Pour faire une demande de transfert :

1. Cliquez sur **Accueil > Mon bureau > Questionnaires et check-lists > Mes questionnaires d'évaluation**.

   ☛ *Dans certaines solutions, le menu est : **Accueil > Mon bureau > Mes responsabilités > Mes questionnaires d'évaluation**.*

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

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

   ☛ *Les demandes de transfert sont exceptionnelles si le travail préparatoire à la création de la campagne d'exécution a été correctement réalisé.*

SUIVRE L'AVANCEMENT DES QUESTIONNAIRES

Consulter les résultats de la session

Pour consulter l'avancement d'une session d'évaluation :

- Ouvrez la page de propriétés de la session d'évaluation et cliquez sur l'onglet **Rapports > Suivi**.

  ☛ *Pour accéder à la session, voir "Accéder aux sessions d'évaluation", page 55.*

Visualiser les questionnaires envoyés

Pour accéder à la liste des questionnaires envoyés :

- Cliquez sur **Gestion des campagnes > Campagnes > Suivi > Questionnaires envoyés**.

Valider les questionnaires d'évaluation

Pour accéder à la liste des questionnaires d'évaluation remplis par les répondants :

1. Cliquez sur **Gestion des campagnes > Campagnes > Suivi > Questionnaires remplis**.
   La liste des questionnaires remplis apparaît.
   Vous pouvez constater que le statut de workflow est passé à "A valider".
2. Sélectionnez le questionnaire qui vous intéresse et cliquez sur le bouton **Afficher les questionnaires**.
   Le contenu du questionnaire apparaît dans un nouvel onglet. Vous pouvez visualiser les réponses.
3. Fermez la fenêtre d'affichage du questionnaire.
4. Si vous estimez que le questionnaire a été rempli correctement, cliquez sur son icône et sélectionnez **Questionnaire d'évaluation (A valider) > Valider**.
   Le questionnaire est fermé et les résultats sont calculés automatiquement.

Demander à un répondant de modifier ses réponses

Si les réponses à un questionnaire ne conviennent pas, vous pouvez demander au répondant de le modifier.

Pour faire une demande de modification :

1. Cliquez sur **Gestion des campagnes > Campagnes > Suivi > Questionnaires remplis**.
2. Cliquez sur l'icône du questionnaire et sélectionnez **Questionnaire d'évaluation (A valider) > Demander une modification.**

> ☛ *Le répondant peut modifier ses réponses. Voir "Remplir les questionnaires", page 66.*

Réassigner un questionnaire

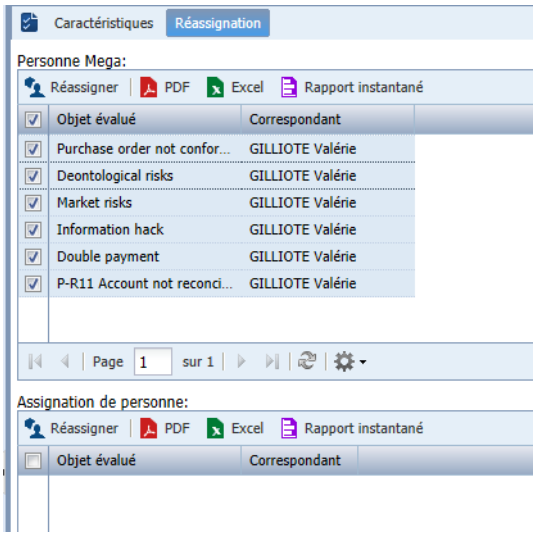
Si un répondant a fait une demande de transfert, vous devez réassigner le questionnaire.

Pour réassigner un questionnaire :

1. A partir de la liste des questionnaires envoyés, sélectionnez le questionnaire qui vous intéresse.

> ☛ *Les questionnaires sont accessibles depuis des menus différents selon le bureau utilisé :*
>
> - *Dans le cadre d'une solution **MEGA**, vous pouvez accéder aux questionnaires à partir de l'onglet de navigation **Gestion des campagnes**.*
> - *Dans le bureau du gestionnaire d'évaluation, les questionnaires sont accessibles depuis la fenêtre de navigation **Mes questionnaires**.*

2. Ouvrez la fenêtre de propriétés du questionnaire concerné et sélectionnez l'onglet **Réassignation**.



> ☛ *Cet onglet apparaît seulement lorsque le questionnaire a pour statut "A réassigner".*

3. Sélectionnez l'ensemble des noeuds à évaluer et cliquez sur le bouton **Réassigner**.

4. Grâce à la fenêtre de recherche qui s'ouvre, sélectionnez la personne chargée de répondre au questionnaire et cliquez sur **OK**.

   ☛ *Si des assignations de personne ont été spécifiées (par exemple, le questionnaire est à envoyer à une personne dans le cadre d'un rôle métier en particulier), vous pouvez réassigner le questionnaire dans la section prévue à cet effet.*

   Le nouveau répondant apparaît dans la colonne **Correspondant**.
5. Cliquez sur l'icône du questionnaire et sélectionnez **Questionnaire d'évaluation (A réassigner) > Réassigner**.

Le nouveau répondant reçoit un e-mail. Il peut remplir le questionnaire, dont le statut est de nouveau "En cours" puis soumettre ses réponses.

FERMER LA SESSION D'ÉVALUATION

Vous pouvez à tout moment fermer la session.

Pour fermer une session d'évaluation :

1. Ouvrez la fenêtre de propriétés de la campagne et sélectionnez l'onglet **Session**.

   ☛ *Pour accéder à la campagne, voir "Accéder aux campagnes d'évaluation", page 54.*

2. Dans la section **Session d'évaluation**, cliquez sur l'icône de la session qui vous intéresse et sélectionnez **Fermer**.
   Tous les questionnaires sont fermés automatiquement. Cette opération peut prendre quelques minutes.

   ☛ *Les résultats sont considérés comme valides uniquement si la session est fermée.*

TRAITER LES RISQUES

Dans une optique d'amélioration continue l'entreprise doit mener des actions pour éliminer les causes de non-conformités aux exigences informatiques afin d'éviter qu'elles ne se reproduisent.

HOPEX IT Risk Management vous permet de spécifier, de mettre en œuvre et de suivre des plans d'action définis pour traiter les risques. Traiter les risques consiste également à sélectionner et mettre en œuvre des contrôles visant à diminuer le risque.

Le IT RM Manager définit les plans d'action de maîtrise des risques informatiques, et alloue les actions aux propriétaires d'application responsables de leur mise en œuvre.

✓ "Mode de traitement des risques", page 74
✓ "Gérer les plans d'action", page 76

☛ *Pour plus de détails sur les plans d'action, voir le guide **HOPEX Collaboration Manager**.*

MODE DE TRAITEMENT DES RISQUES

Pour spécifier les choix de traitement d'un risque :

❱ Dans la page de propriétés du risque, sélectionnez la page **Traitement**.

☛ *Pour accéder aux risques, voir "Accéder aux risques", page 28.*

Modes de traitement

Diverses solutions permettant de faire face au risque sont proposées.

- ***Acceptation***
  Il s'agit de la stratégie de gestion du risque qui consiste en la décision éclairée d'accepter le risque. Tant qu'aucune volonté de traitement du risque ne se manifeste, cette stratégie ne permet pas de protéger l'organisation contre le risque.
- ***Réduction***
  Il est possible de réduire la fréquence du risque, en mettant en place des contrôles supplémentaires ou de réduire l'impact de ses conséquences si le risque survient.
- ***Transfert*** (sous-traitant)
  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 fréquence est faible, mais l'impact élevé. Dans ce cas, l'assureur demande généralement que des mesures de prévention et de réduction du risque soient également mises en place.

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

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

Niveaux de risque

Le choix du traitement doit porter sur une solution ramenant le **Risque résiduel** en deçà du seuil de tolérance souhaité par la direction.

Dans le champ **Risque cible**, vous pouvez indiquer le niveau de risque accepté par l'organisation.

Spécifier les contrôles et actions à mettre en œuvre

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 œuvre pour les maîtriser. On précisera également quels sont les contrôles mis en place pour prévenir le risque, ainsi que les procédures curatives à mettre en œuvre si le risque survient.

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 la page **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.

    ☛ *Pour plus de détails, voir "Gérer les plans d'action", page 76.*
  - L'onglet **Contrôles** dresse la liste des contrôles prévus pour réduire le risque.

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

GÉRER LES PLANS D'ACTION

Créer un plan d'action

Pour créer un plan d'action :

1. Cliquez dans le menu de navigation principal puis sur **Inventaires**.
2. Cliquez sur **Traitement > Plans d'action**.
3. Cliquez sur **Nouveau**.
   Le plan d'action est créé.

Vous pouvez renseigner les caractéristiques du plan d'action dans sa fenêtre de propriétés. Voir "Caractériser le plan d'action", page 76.

Caractériser le plan d'action

Pour renseigner les propriétés d'un plan d'action :

1. Cliquez dans le menu de navigation principal puis sur **Inventaires**.
2. Cliquez sur **Traitement > Tous les plans d'action**.
3. Ouvrez la fenêtre de propriétés du plan d'action désiré.

Caractéristiques générales

Vous pouvez spécifier les informations suivantes :

- **Nom** : nom du plan d'action
- **Propriétaire** : ce champ est renseigné par défaut par l'utilisateur qui crée le plan d'action.
- **Entité propriétaire** : entité responsable de la mise en œuvre du plan d'action.
- **Approbateur** : utilisateur responsable de la validation du plan d'action quand toutes les actions sont terminées.
- **Moyens** : description textuelle des moyens nécessaires /souhaités pour l'exécution du plan d'action.
- **Priorité du plan d'action**: permet d'indiquer un niveau. La priorité peut être :
  - "Basse"
  - "Moyenne"
  - "Elevée"
  - "Critique".
- **Origine** : permet de définir le contexte de réalisation du plan d'action :
  - "Audit"
  - "Conformité"
  - "Evénement"
  - "Risque"
  - "RFC"
  - "Autre".
- **Catégorie** : le plan d'action peut par exemple être lié à :
  - la réduction de l'impact des risques
  - la gestion de projet
  - l'amélioration des processus
  - l'amélioration de la performance des contrôles
  - etc.

    ☛ *De nombreuses autres valeurs sont disponibles.*
- **Nature** : permet de définir s'il s'agit d'un plan d'action :
  - Correctif
  - Préventif.
- **Commentaires** : permet d'apporter un complément d'information sur le plan d'action et ses caractéristiques.
- **Calendrier de pilotage** : permet d'envoyer des rappels à la personne responsable d'un plan d'action afin qu'elle renseigne le taux d'avancement de ce plan d'action.

  ☛ *Un calendrier de pilotage pour un rappel mensuel d'avancement est fournir par défaut.*

Analyse financière

- **Coût prévu** : estimation du coût du plan d'action
- **Coût prévu (Jour-Homme)** : estimation exprimée en jours.homme de la charge nécessaire à la mise en œuvre du plan d'action

RACI

L'utilisateur défini comme **Réalisateur** du plan d'action est responsable de la définition des actions à réaliser ainsi que de leur réalisation.

Ce champ est renseigné par l'utilisateur qui crée le plan d'action ou par l'approbateur du plan d'action.

☛ *Pour plus de détails sur l'utilisation du RACI, voir "Responsabilités", page 24.*

Facteurs de succès

Dans la section **Facteurs clés de succès**, vous pouvez renseigner de manière textuelle des indicateurs de succès qui permettront de juger de la réussite du plan d'action.

Périmètre

Pour positionner un plan d'action dans son environnement, vous pouvez associer des objets à ce plan d'action dans la section **Périmètre**.

Vous pouvez relier des objets des types suivants :

- contrôles
- applications
- risques
- entités
- processus
- incidents

Jalons

Les jalons sont des dates clés du plan d'action.

☛ *La date de fin planifiée est obligatoire.*

Pièces jointes

Vous pouvez attacher des documents métier à un plan d'action.

☛ *Pour plus de détails sur l'utilisation des documents métier, voir le guide **HOPEX Common Features**.*

Gérer les actions

Le propriétaire du plan d'action doit définir les actions permettant au plan d'action d'aboutir. Il a la possibilité de créer des actions et les affecter.

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

Pour créer une action à partir d'un plan d'action :

1. Dans le menu de navigation principal cliquez sur **Liste de tâches** puis sur **Mes responsabilités > Mes Plans d'action**.

   ☛ *Selon votre profil, vous pouvez également accéder aux plans d'action via le menu **Traitement > Plans d'action**.*

2. Sélectionnez le plan d'action qui vous intéresse et cliquez sur **Propriétés**.
3. Dans la section **Actions**, cliquez sur **Nouveau**.
4. Dans la page de propriétés de l'action, remplissez les champs :
   - **Priorité** : permet d'indiquer un niveau. La priorité peut être : "Basse", "Moyenne", "Haute" ou "Critique".
   - **Propriétaire** : responsable de l'action tel que désigné par le créateur de l'action.
   - **Entité propriétaire** : entité responsable de la mise en œuvre du plan d'action.
5. Précisez les jalons qui sont les dates importantes de l'action.
   - **Date de début planifiée**
   - **Date de fin planifiée**
6. Cliquez sur **OK**.
   L'action est créée.

Workflows des plans d'action

Selon le profil de la personne qui crée le plan d'action, deux workflows sont disponibles :

- approche "top-down"
- approche "bottom-up"

☛ *Les commandes qui permettent de passer d'un statut de workflow à un autre sont disponibles :*

- *dans le menu contextuel du plan d'action à partir d'une liste de plans d'action*
- *dans la fenêtre de propriétés du plan d'action, en cliquant sur l'icône du plan d'action située en haut à gauche*

Approche "bottom-up"

Dans une approche "bottom-up", le plan d'action est créé par un utilisateur quelconque (par exemple Propriétaire d'application ou IT RM Manager. Un approbateur doit valider le plan d'action pour que celui-ci puisse être mis en œuvre. C'est le cas lorsque les répondants aux questionnaires d'évaluation proposent un plan d'action : ils doivent d'abord le soumettre via le workflow.

☛ *Pour les différentes étapes du workflow, voir "Workflow de plan d'action "bottom-up"", page 151*

Approche "top-down"

Dans le cadre du workflow "top-down ", le plan d'action est créé par un responsable. Le plan d'action n'a pas besoin d'être validé dans ce cas.

☛ *Pour les différentes étapes du workflow, voir "Workflow de plan d'action "top-down"", page 152.*

Workflow des actions

Une fois que les actions d'un plan d'action sont définies, le fait de démarrer le plan d'action démarre les actions liées.

Une fois que le responsable d'action a terminé ses actions, il peut fermer ces dernières. La fermeture du plan d'action ferme automatiquement les actions liées.

☛ *Voir "Workflow d'actions", page 153*

Suivre les plans d'action

Renseigner l'avancement d'un plan d'action

Vous pouvez créer des états d'avancement de manière à rendre compte de son avancement.

Pour renseigner l'avancement du plan d'action :

1. A partir du menu de navigation, cliquez sur **Traitement > Plans d'action**.
2. Sélectionnez un plan d'action et ouvrez sa fenêtre de propriétés.
3. Dépliez la section **Avancement du plan d'action** et dans le cadre **Etat d'avancement** cliquez sur **Nouveau**.
4. Spécifiez un **Pourcentage d'avancement**.
5. Donnez éventuellement une **Evaluation de l'avancement**.
   Vous pouvez préciser si le plan d'action est :
   - dans les temps
   - en retard
6. Cliquez sur **OK**.
   L'état d'avancement est créé. Vous pouvez en créer à intervalle régulier.

Rapports de suivi des plans d'action

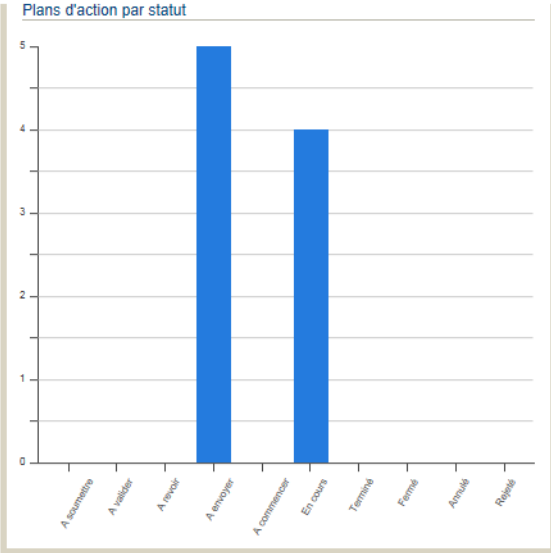
Un rapport vous permet de suivre les plans d'action.

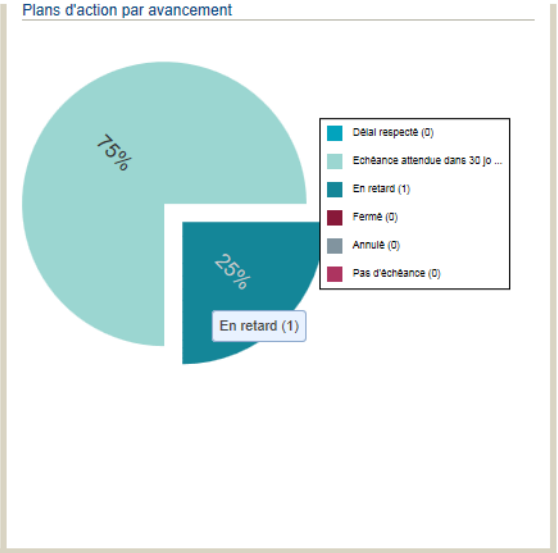
Pour y accéder :

1. Depuis le menu de navigation, cliquez sur **Traitement > Plans d'action > Rapport de suivi**.
2. Cliquez sur **Créer**.

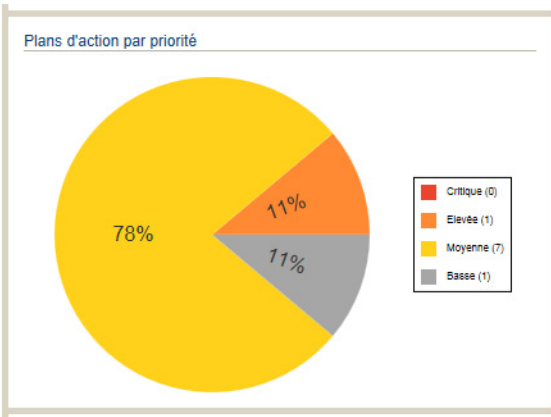
   ☛ *Vous pouvez éventuellement renseigner des paramètres dans l'onglet correspondant.*

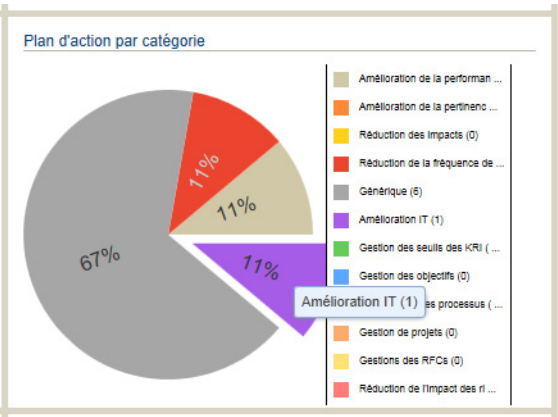
3. Cliquez sur l'onglet **Rapports** pour voir le résultat apparaître.
   Ce rapport présente plusieurs diagrammes à barres / circulaires représentant la répartition des plans d'action
   - par statut
   - par avancement



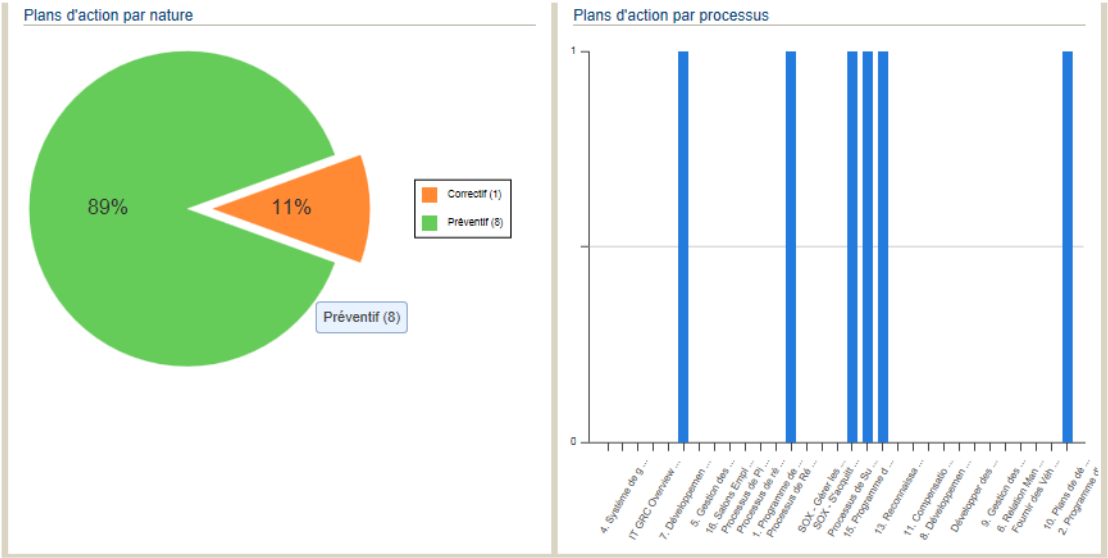


   - par priorité
   - par catégorie

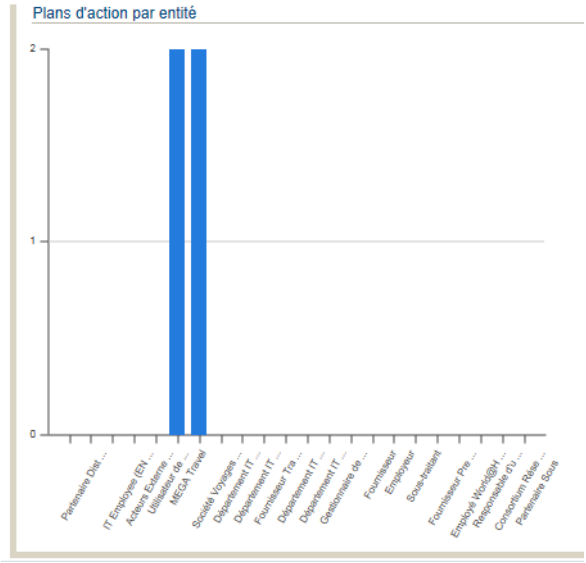




- par nature
- par processus



- par entité



Pour accéder aux plans d'action concernés :

1. Cliquez dans la barre ou le secteur de diagramme qui vous intéresse.
2. Les plans d'action correspondant apparaissent sous forme de liste en bas de la page.

RAPPORTS DE HOPEX IT RISK MANAGEMENT

Ce chapitre décrit les rapports utilisés dans le cadre de la solution **HOPEX IT Risk Management**.

✓ "Accéder aux rapports", page 84
✓ "Rapports concernant les risques informatiques", page 86
✓ "Rapports concernant la conformité informatique", page 97
✓ "Rapports concernant la gestion des fournisseurs", page 105
✓ "Rapports concernant les évaluations", page 107

Les résultats des rapports peuvent être différents en fonction du modèle d'évaluation sélectionné.

☛ *Pour personnaliser les rapports, voir le guide **HOPEX Common Features**, chapitre "Générer la documentation avec HOPEX", "Personnaliser vos rapports".*

ACCÉDER AUX RAPPORTS

Il existe différentes manières d'accéder aux rapports dans **HOPEX IT Risk Management**.

Accéder à l'onglet dédié aux rapports

Un grand nombre de rapports sont disponibles dans un onglet prévu à cet effet.

Pour y accéder :

1. Ouvrez le bureau **HOPEX IT Risk Management**.
2. Depuis le menu de navigation principal, cliquez sur **Rapports**.
   Vous accédez aux rapports classés par thématique :
   - "Rapports concernant les risques informatiques", page 86
   - "Rapports concernant la conformité informatique", page 97
   - "Rapports concernant la gestion des fournisseurs", page 105

Accéder aux rapports disponibles directement sur les objets

En-dehors des rapports listés dans l'onglet dédié, des rapports sont disponibles :

- directement sur les objets
- dans les différents menus de la solution, notamment sous forme de matrices permettant également de modifier le référentiel

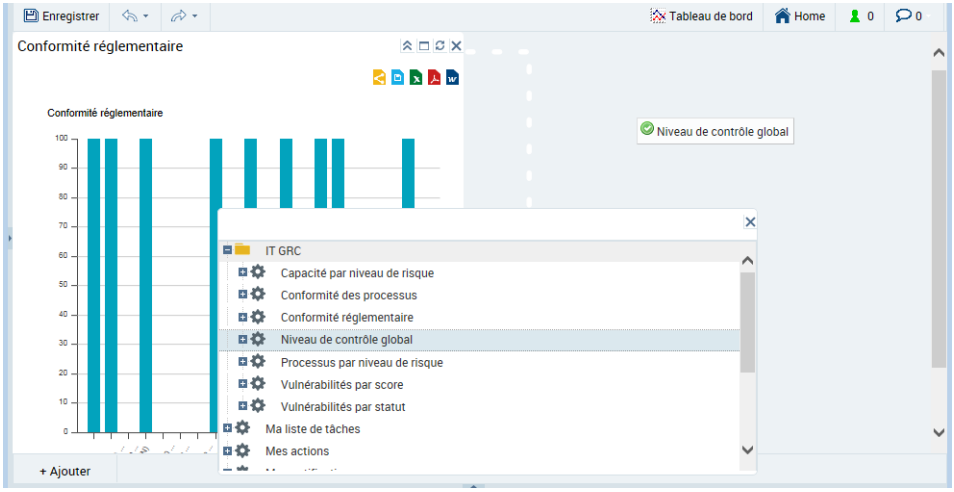
Accéder aux widgets

Vous pouvez facilement ajouter des widgets dans votre tableau de bord.

Pour ajouter un widget :

1. Depuis le menu de navigation principal, cliquez sur **Tableau de bord** puis en bas à gauche sur **Ajouter**.

2. Dans la fenêtre qui apparaît, sélectionnez le widget que vous souhaitez ajouter et faites un glisser-déposer sur votre bureau.



RAPPORTS CONCERNANT LES RISQUES INFORMATIQUES

☛ *Pour plus de détails sur la gestion des risques, voir "Gérer les risques informatiques", page 36.*

Rapports concernant l'identification des risques

Criticité des applications

Chemin d'accès

Rapports > Risques informatiques > Identification > Criticité des applications

Paramètres

- Processus métier : liste de 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.*

- Type d'application (facultatif)

Résultat

Ce rapport présente sous formes de bulles les applications reliées aux processus métier, avec les indications suivantes :

En abscisses	Nombre d'applications interfacées via des flux avec l'application considérée
En ordonnées	Nombre de capacités métier reliées à l'application
Taille des bulles	Nombre d'installations logicielles de l'application
Couleur de la bulle	Fonction du coût global de l'application

📖 *Une capacité métier est une unité de découpage des traitements d'un système d'information. Les traitements peuvent par exemple correspondre à une activité ou à un métier de l'entreprise.*

☛ *Le coût global de l'application est disponible dans la solution **HOPEX IT Portfolio Management**.*

Exemple

Tableau Menaces et Vulnérabilités

Chemin d'accès

Rapports > Risques informatiques > Identification > Tableau Menaces et vulnérabilités

Paramètres

- Dates de début et de fin

  ☛ *Les dates de début et de fin permettent de définir la plage de valeur à prendre en compte pour les évaluations. Si le même objet est évalué plusieurs fois durant la période, c'est la dernière évaluation qui est retenue.*

- Menaces exploitant les vulnérabilités

  📖 *Les menaces sont des facteurs externes ou internes qui mettent en danger les actifs informatiques de l'entreprise.*

  📖 *Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif.*

Résultat

Le rapport présente les risques via l'arborescence Menace > Vulnérabilité > Application.

Il affiche la dernière évaluation des risques pour le contexte de l'application.

Exemple

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

Rapports concernant les actifs informatiques

Niveau de risque agrégé par processus métier

Chemin d'accès

Rapports > Risques informatiques > Actifs informatiques > Niveau de risque agrégé par processus métier

Paramètres

- Dates de début et de fin

  ☛ *Les dates de début et de fin permettent de définir la plage de valeur à prendre en compte pour les évaluations. Si le même objet est*

évalué plusieurs fois durant la période, c'est la dernière évaluation qui est retenue.

- Modèle d'évaluation :
  - pour les applications
  - pour les installations

> ☛ *Pour plus de détails sur les modèles d'évaluation, voir "Modèles d'évaluation des risques", page 43.*

- 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.*

Le bouton **Générer agrégation** permet de lancer le calcul et de consolider les évaluations des risques sur les applications et les processus.

Résultat

Ce rapport se présente sous la forme d'une arborescence "Processus métier > Application > Risques".

Le résultat de l'évaluation est affiché pour chaque élément de l'arborescence.

Exemple

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

Heatmap des risques

Chemin d'accès

Rapports > Risques informatiques > Actifs informatiques > Heatmap des risques

Paramètres

- Date de début et de fin

  ☛ *Ces dates permettent de définir la plage de valeur à prendre en compte pour les évaluations. Si le même objet est évalué plusieurs fois durant la période, c'est la dernière évaluation qui est retenue.*

- Risques : permet de sélectionner les risques en les filtrant grâce à différents critères.

Vous pouvez sélectionner les risques à prendre en compte via des arborescences.

Critère de sélection des risques	Arborescence de sélection correspondante
Ligne métier	Lignes métier > Applications > Risques
Risque type	Risques types > Risques
Processus	Processus > Applications > Risques
Capacité métier	Capacités métier > Applications > Risques
Menaces	Menaces > Vulnérabilités > Applications > Risques

Résultat

Les heatmaps illustrent les caractéristiques suivantes :

- Impact / Probabilité

  🕮 *L'impact caractérise l'impact du risque lorsqu'il se manifeste.*

  🕮 *La probabilité caractérise la probabilité que le risque se manifeste.*

- Risque inhérent / Vélocité

  🕮 *Le risque inhérent (ou brut) désigne le risque auquel l'organisation est exposée en l'absence de mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque. Il s'agit du produit de la valeur de l'impact par la valeur de la probabilité avant prise en compte des mesures de prévention ou d'atténuation du risque.*

  🕮 *La vélocité représente la rapidité de propagation d'un risque depuis un actif sur les autres actifs si un incident survient.*

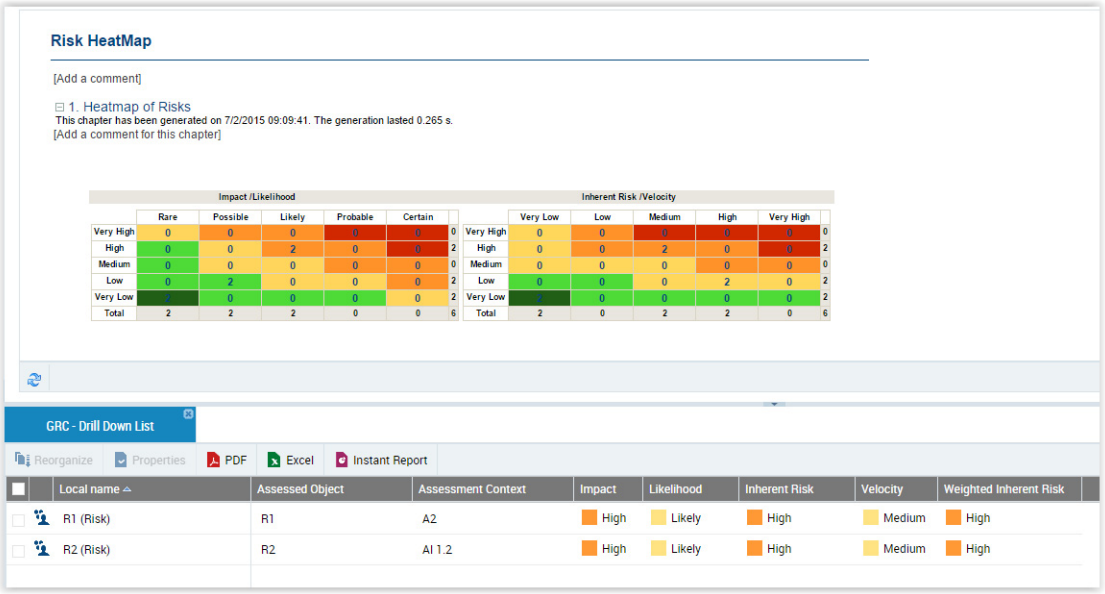
Les valeurs de chaque cellule représentent les évaluations des risques sélectionnés.

☛ *Par défaut tous les risques sont pris en compte.*

Pour visualiser les évaluations correspondant à chaque cellule :

❱ Cliquez sur la valeur de la cellule.
Les évaluations apparaissent, avec comme indication le risque évalué et son contexte (application ou installation logicielle).

Exemple



Heatmap des applications

Chemin d'accès

Rapports > Risques informatiques > Actifs informatiques > Heatmap des applications

Paramètres

- Date de début et de fin

  ☛ *Les dates de début et de fin permettent de définir la plage de valeur à prendre en compte pour les évaluations. Si le même objet est évalué plusieurs fois durant la période, c'est la dernière évaluation qui est retenue.*

- Applications : permet de sélectionner les applications à prendre en compte, en se basant sur différents critères et arborescences.

Critère de sélection des applications	Arborescence de sélection correspondante
Processus	Processus > Applications
Ligne métier	Ligne métier > Applications
Capacité métier	Capacité métier > Applications

Résultat

Les heatmaps illustrent les caractéristiques suivantes :

- Risque inhérent / Vélocité

  Le risque inhérent (ou brut) désigne le risque auquel l'organisation est exposée en l'absence de mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque. Il s'agit du produit de la valeur de l'impact par la valeur de la probabilité avant prise en compte des mesures de prévention ou d'atténuation du risque.

  La vélocité représente la rapidité de propagation d'un risque depuis un actif sur les autres actifs si un incident survient.

- Impact / Probabilité

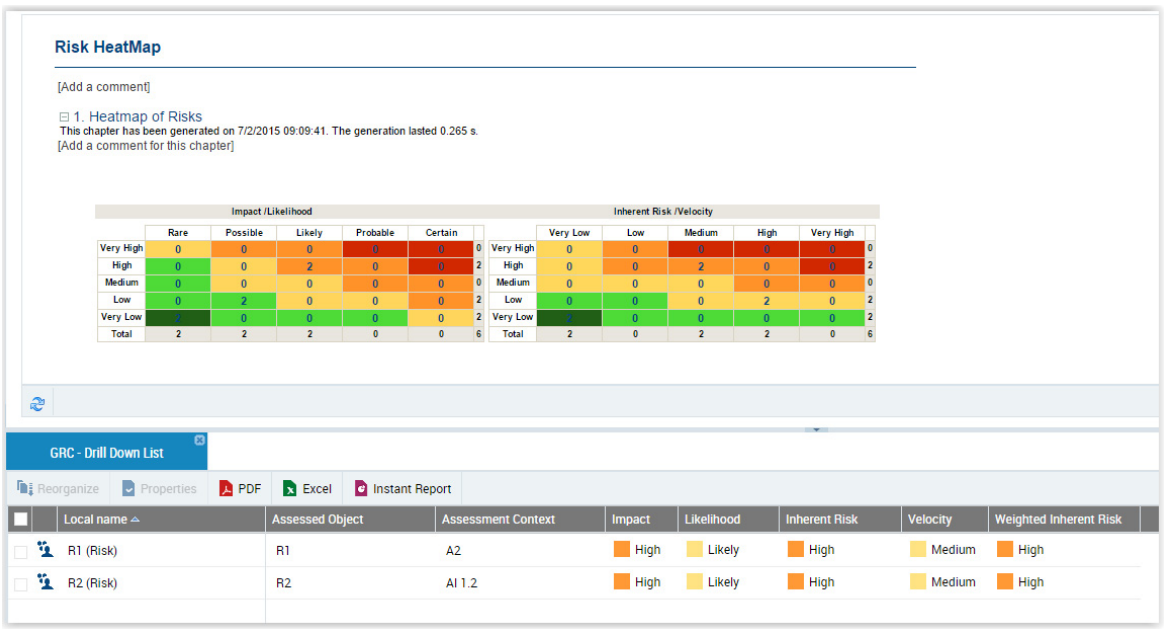
  L'impact caractérise l'impact du risque lorsqu'il se manifeste.

  La probabilité caractérise la probabilité que le risque se manifeste.

Les valeurs de chaque cellule représentent le niveau de risque moyen de l'application.

Vous pouvez visualiser les évaluations concernant les applications en cliquant sur la valeur de la cellule.

Exemple



Widgets concernant les risques

Les widgets sont accessibles depuis le tableau de bord via la page d'accueil.

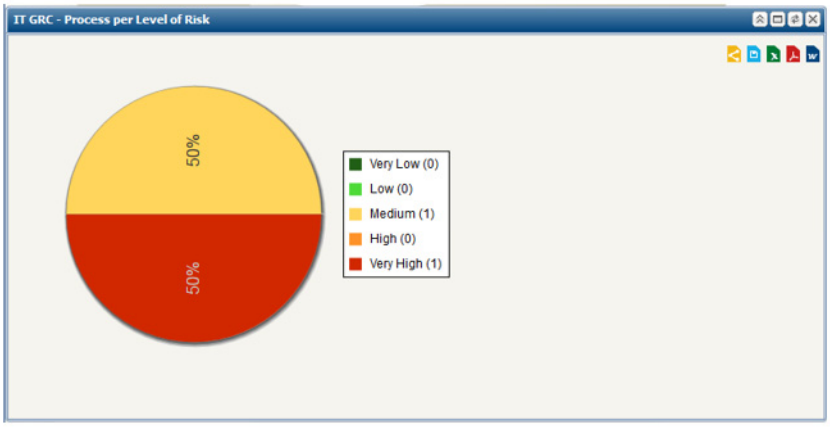
Ils ne contiennent pas de paramètres.

Widget Processus par niveau de risque

Ce widget permet d'afficher le pourcentage de processus métier de premier niveau en fonction de la valeur du risque inhérent moyen pour le processus.

☛ *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.*

Le risque inhérent (ou brut) désigne le risque auquel l'organisation est exposée en l'absence de mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque. Il s'agit du produit de la valeur de l'impact par la valeur de la probabilité avant prise en compte des mesures de prévention ou d'atténuation du risque.

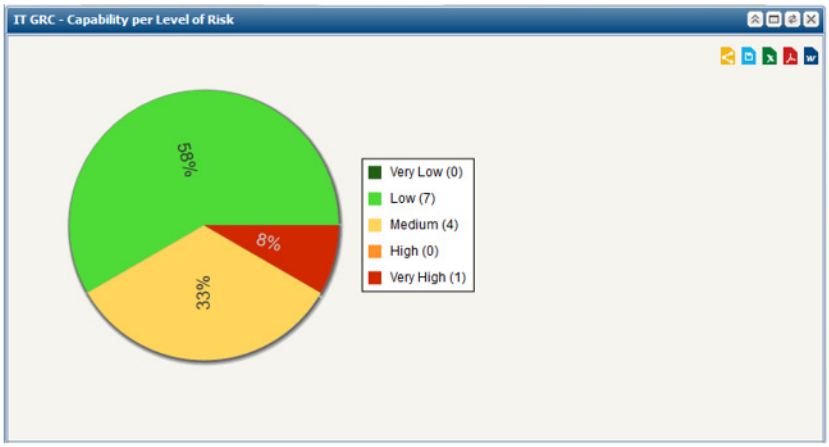


Vous pouvez visualiser les processus correspondants en cliquant sur la zone qui vous intéresse.

Widget Capacités par niveau de risque

Diagramme sectoriel affichant le pourcentage du nombre total de capacités de premier niveau par niveau de risque.

☛ *Une capacité métier est une unité de découpage des traitements d'un système d'information. Les traitements peuvent par exemple correspondre à une activité ou à un métier de l'entreprise.*



Rapport de causalité de risques

Voir "Rapport de causalité de risques", page 40.

Rapports concernant les vulnérabilités

Des widgets concernant les vulnérabilités sont fournis en standard.

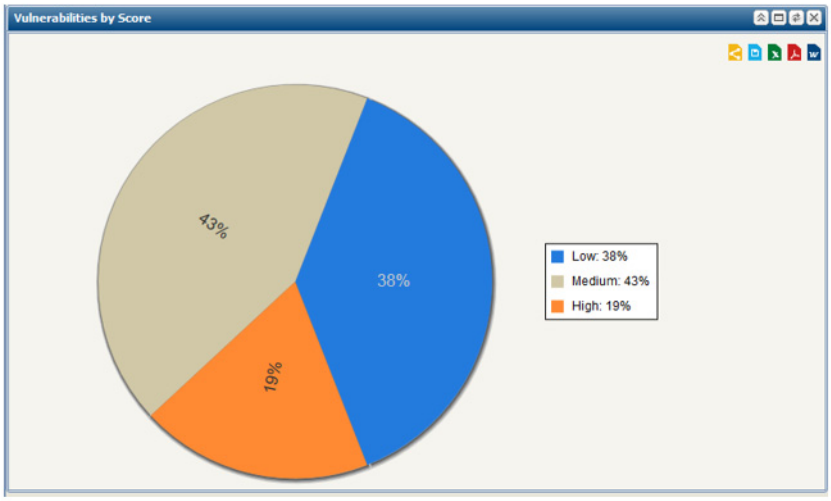
Widget Vulnérabilité par score

Diagramme sectoriel affichant le nombre de vulnérabilités par score :

- bas
- moyen
- haut

> 🕮 *Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent*

conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif.



Vous pouvez visualiser les vulnérabilités correspondantes en cliquant sur la zone qui vous intéresse.

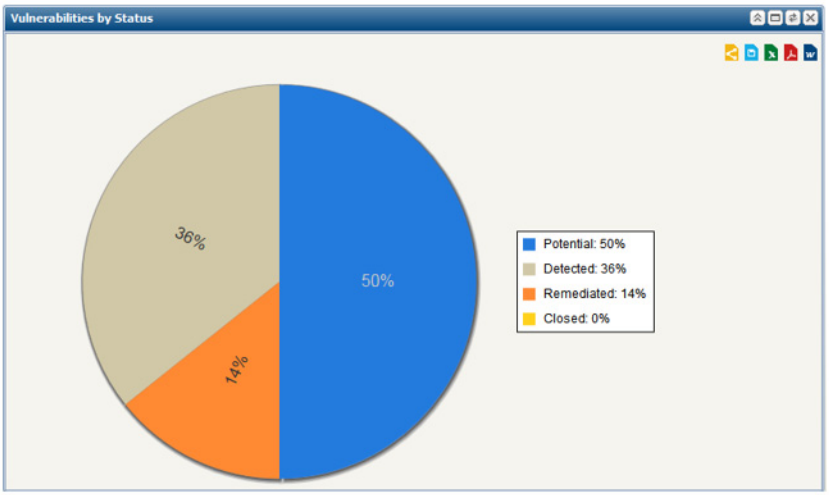
Widget Vulnérabilité par statut

Diagramme sectoriel affichant le nombre de vulnérabilités par statut :

- potentiel
- détecté
- traité
- fermé

> 🕮 *Les vulnérabilités sont des défauts de maîtrise d'un actif (informatique) qui le rendent vulnérable à une menace et peuvent*

conduire à un défaut de confidentialité, d'intégrité ou de disponibilité de cet actif.



Vous pouvez visualiser les vulnérabilités correspondantes en cliquant sur la zone qui vous intéresse.

RAPPORTS CONCERNANT LA CONFORMITÉ INFORMATIQUE

☛ *Pour plus de détails, voir "Gérer la conformité informatique", page 44.*

Identification des contrôles

Ce rapport présente la répartition des contrôles sur plusieurs axes :

- par processus

  ☛ *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.*

- par type de contrôle

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

- par entité

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

- par objectif

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

- par cadre réglementaire

  🕮 *Une réglementation ou 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 de politiques internes.*

Chemin d'accès

Rapports > Conformité informatique > Identification des contrôles

Paramètres

Il s'agit ici de sélectionner les contrôles présentés en précisant les éléments qui définissent leur périmètre :

- les types de contrôle
- les entités
- les processus
- les objectifs

Paramètres	Type du paramètre	Contraintes
Date de début	date	Critère de sélection des évaluations. Non obligatoire.
Date de fin	date	Critère de sélection des évaluations ; fixée à la date courante.
Type de contrôle du périmètre	type de contrôle	Critère de sélection des contrôles. Non obligatoire.
Entités du périmètre	entité	Critère de sélection des contrôles. Non obligatoire.
Processus du périmètre	processus	Critère de sélection des contrôles. Non obligatoire.
Objectifs du périmètre	objectifs	Critère de sélection des contrôles. Non obligatoire.

Résultat

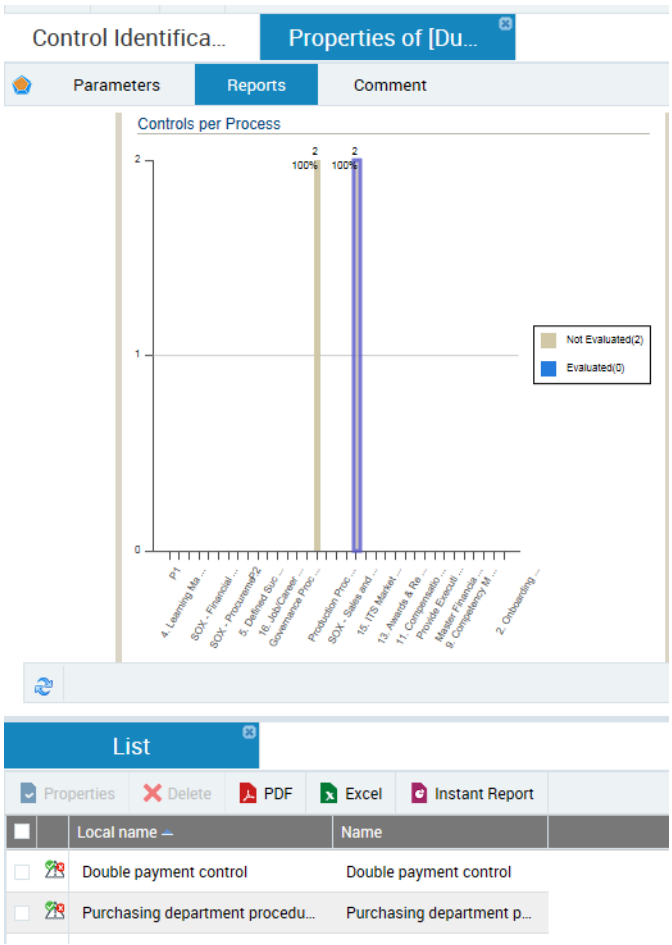
Le rapport présente la répartition des contrôles sous forme d'un diagramme empilé. Les critères de répartition sont les suivants :

- Répartition par processus
- Répartition par type de contrôle
- Répartition par entité
- Répartition par objectif
- Répartition par statut
- Répartition par cadre réglementaire

Exemple

Le graphique ci-dessous montre le nombre de contrôles (évalués ou non) par réglementation.

Lorsque vous cliquez sur une barre du graphique, les contrôles concernés apparaissent dans une liste en bas de la page.



Niveau de contrôle par réglementation

Le niveau de contrôle caractérise le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour évaluer le risque.

Chemin d'accès

Rapports > Conformité informatique > Niveau de contrôle par réglementation

Paramètres

- Date de fin : date du jour, par défaut
- Date de début : date correspondant à la date de fin mais l'année précédente
- Réglementations : ensemble de réglementations servant à filtrer les contrôles (obligatoire)

  Une réglementation ou 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 de politiques internes.
- Processus (facultatif)

  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.

Le bouton **Générer l'agrégation** permet de lancer les calculs.

Résultat

Ce rapport se présente sous la forme d'une arborescence qui affiche une évaluation pour chaque élément de la branche. La branche s'articule de la manière suivante :

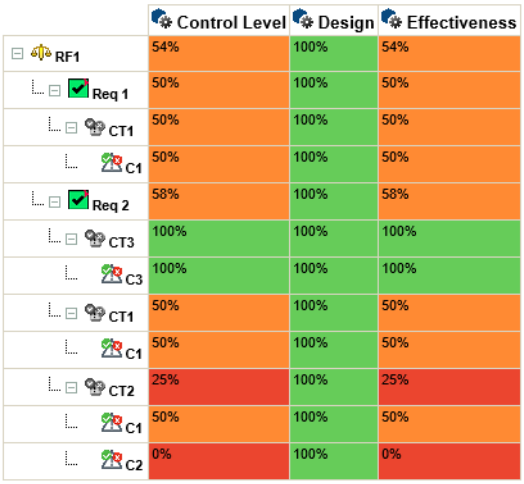
```
Cadre réglementaire > Exigences > Types de contrôle >
Contrôles
```

Voici la signification de chaque ligne :

Ligne	Affichage
Contrôles	Moyenne de l'évaluation du contrôle (%) pour l'ensemble des applications reliées.
Types de contrôles	Moyenne de l'évaluation pour les contrôles du type

Un contrôle appartenant à différents types est "compté" plusieurs fois.

Exemple



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

Niveau de contrôle par processus métier

Le niveau de contrôle caractérise le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour évaluer le risque.

Chemin d'accès

Rapports > Conformité informatique > Niveau de contrôle par processus métier

Paramètres

- Date de fin : date du jour, par défaut
- Date de début : date correspondant à la date de fin mais l'année précédente
- Processus (obligatoire)
- Réglementations : permet de filtrer les contrôles à prendre en compte (facultatif)

Le bouton **Générer l'agrégation** permet de lancer les calculs.

Résultat

Ce rapport se présente sous la forme d'une arborescence affichant la moyenne de la dernière évaluation pour chaque élément de l'arbre.

L'arborescence est de ce type : Processus métier > Applications > Contrôles.

La ligne concernant le contrôle donne la dernière évaluation élémentaire du contrôle dans le contexte de l'application.

Exemple

	Control Level	Design	Effectiveness
Billing	100%	100%	100%
PayIT	100%	100%	100%
Sensitive outbound Application Communications are cyphered	Pass	Adequate	Effective
Purchase Goods or Services	50%	50%	100%
BuyIT	50%	50%	100%
Access Controls to ERP are reviewed each quarter	Fail	Inadequate	Effective
encrypted VPN access tunnels are used for inbound access to ERP	Pass	Adequate	Effective

Widgets concernant la conformité

Les widgets sont accessibles depuis le tableau de bord via la page d'accueil.

Ils ne contiennent pas de paramètres.

Conformité des processus

Diagramme à barres présentant le niveau de contrôle moyen des processus racines.

Le niveau de contrôle caractérise le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour évaluer le risque.

Pour accéder aux applications du processus :

- Cliquez sur la barre correspondante.
  Vous obtenez la liste des applications du processus avec leur taux de conformité moyen.

Conformité réglementaire

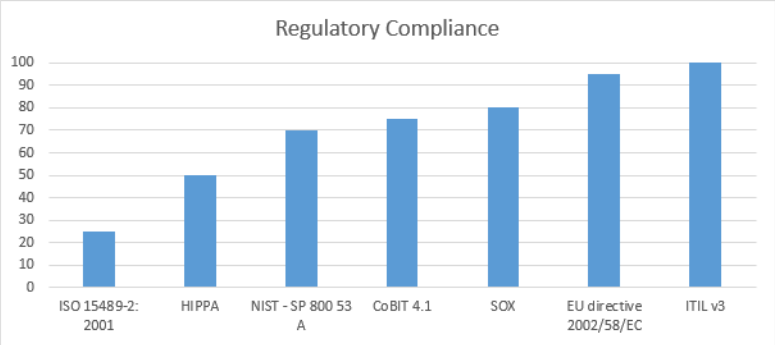
Diagramme à barres présentant :

- en abscisses : les cadres réglementaires racines

  📖 *Une réglementation ou 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 de politiques internes.*

- en ordonnées : le niveau de contrôle moyen

  📖 *Le niveau de contrôle caractérise le niveau d'efficacité des éléments de maîtrise déployés (contrôles) pour évaluer le risque.*



Pour accéder aux exigences du cadre réglementaire :

1. Cliquez sur la barre correspondante.

   ☛ *Les éventuels sous-cadre réglementaires ne sont pas affichés.*

Vous obtenez la liste des exigences du cadre réglementaire avec leur taux de conformité.

📖 *Le taux de conformité est le pourcentage de contrôles satisfaisants par cadre réglementaire racine.*

Pour plus de détails sur l'obtention du taux de conformité, voir "Evaluation directe des risques", page 42

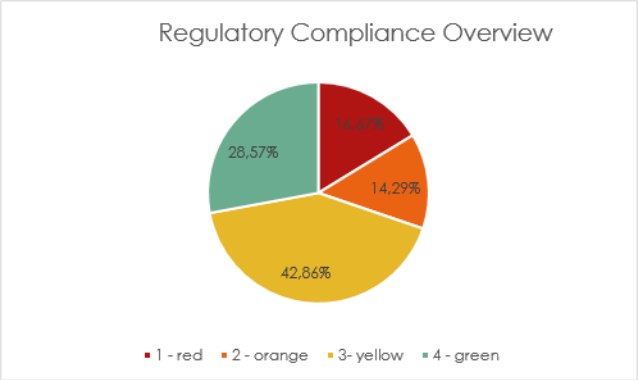
Niveau de contrôle global

Diagramme circulaire synthétisant la ventilation des cadres réglementaires par niveau de conformité.

📖 *Le taux de conformité est le pourcentage de contrôles satisfaisants par cadre réglementaire racine.*

📖 *Une réglementation ou 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 de politiques internes.



Pour afficher la liste des cadres réglementaires d'un secteur du diagramme :

- Cliquez sur le secteur concerné.

Pour plus de détails sur l'obtention du taux de conformité, voir "Evaluation directe des risques", page 42.

RAPPORTS CONCERNANT LA GESTION DES FOURNISSEURS

☛ *Pour plus de détails sur la gestion des fournisseurs, voir "Gérer les fournisseurs informatiques", page 48.*

Matrice Fournisseur par type x Niveau de risque

Chemin d'accès

Rapports > Gestion des fournisseurs informatiques > Fournisseur par type X Niveau de risque

Paramètres

N/A

Résultats

Ce rapport présente le nombre de fournisseurs par niveau de risque et type de fournisseur. Il permet d'accéder à la liste des fournisseurs.

Pour accéder aux fournisseurs :

❱ Cliquez sur le chiffre apparaissant dans les cellules.
Les informations suivantes sont fournies pour chaque fournisseur :

- type de fournisseur
- nom du fournisseur
- évaluation de risque globale
- Montant total des achats (fin de l'année précédente)
- Rang

☛ *Pour plus de détails sur la saisie de ces informations, voir "Caractéristiques des fournisseurs", page 33.*

Exemple

⊟ 1. Matrix Vendor by Vendor Type X Risk Level

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

Niveau de risque fournisseur par ligne métier

Chemin d'accès

Rapports > Gestion des fournisseurs informatiques > Niveau de risque fournisseur par ligne métier

Paramètres

N/A

Résultats

Ce rapport présente le nombre de fournisseurs par niveau de risque et par ligne métier.

Une ligne métier est un haut niveau de classification des principales activités de l'entreprise. Elle correspond, par exemple, à des grands segments produits ou à des canaux de distribution. Elle permet de classifier les processus de l'entreprise, des unités organisationnelles ou des applications qui servent un produit spécifique et/ou un marché spécifique. Les cadres réglementaires de certaines industries imposent leurs propres listes de lignes de métier.

Vous ne pouvez pas accéder à la liste des fournisseurs à partir de ce rapport.

Exemple

1. Risk Level By Business Line

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

RAPPORTS CONCERNANT LES ÉVALUATIONS

☛ *Pour plus de détails sur les évaluations, voir "Evaluations par questionnaires", page 51.*

Suivi des sessions

Chemin d'accès

- Gestion des campagnes > Suivi > Suivi des sessions
- depuis une session d'évaluation.

Pour accéder à ce rapport depuis une session d'évaluation :

1. Dans la page de propriétés d'une campagne d'exécution, cliquez sur l'onglet **Sessions** et ouvrez la page de propriétés d'une session d'évaluation.
2. Cliquez sur l'onglet **Reporting** puis sur **Suivi**.

Paramètres

- session d'évaluation

  Une session d'évaluation est une évaluation lancée sur un laps de temps déterminé. La publication de la session d'évaluation a pour effet d'envoyer un questionnaire d'évaluation contenant les questions aux utilisateurs ciblés.

Résultat

Un résumé affiche des informations générales sur la session d'évaluation courante.

Ce rapport présente plusieurs graphiques concernant l'avancement de la session d'évaluation :

- Pourcentage des questionnaires remplis
- Répartition des questionnaires par statut
- Répartition des questionnaires délégués / non délégués
- Répartition des questionnaires par statut, pour chaque répondant
- Répartition des questionnaires par statut, pour chaque objet évalué

Statistiques des sessions

Ce rapport affiche les données des questionnaires d'une session d'évaluation donnée et permet d'analyser la répartition des réponses.

Chemin d'accès

Gestion des campagnes > Suivi > Statistiques des sessions

Paramètres

Paramètres	Remarques
Campagne	Obligatoire
Session	Obligatoire

Résultat

Une arborescence affiche :

- en ligne : les questions /réponses, ainsi que les répondants
- en colonne : pour chaque question/réponse :
  - le nombre de répondants
  - les objets sur lesquels la réponse porte

  Cette arborescence permet de visualiser qui a répondu quoi pour quelle question.

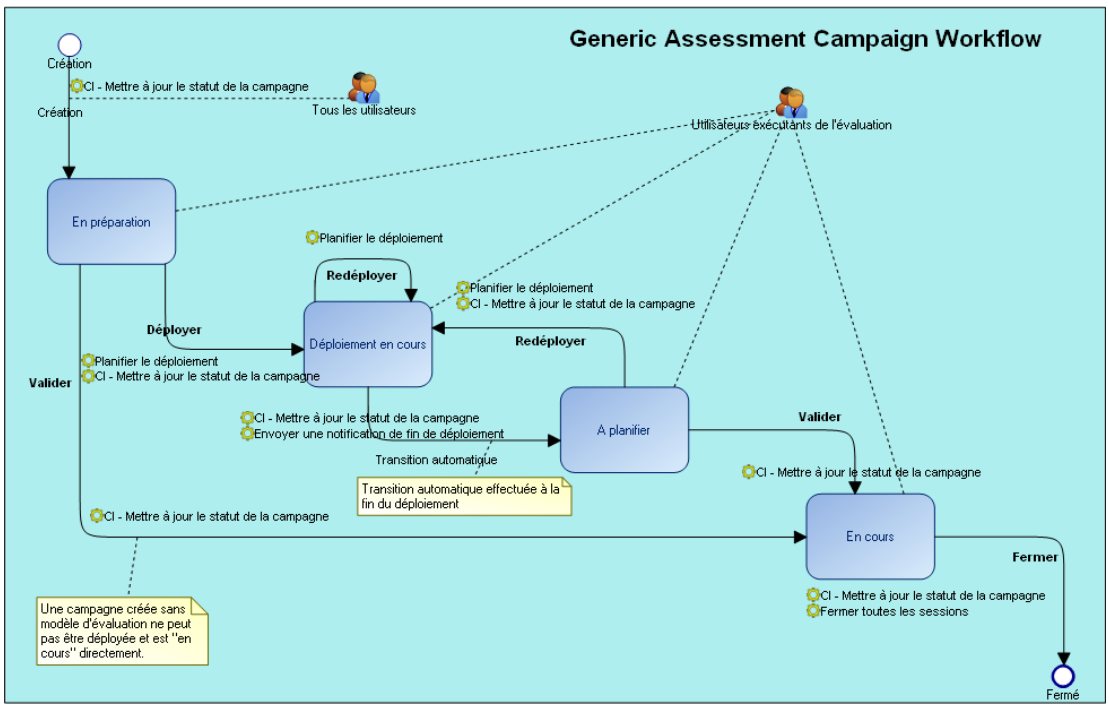
ANNEXE - WORKFLOWS

✓ "Workflow des évaluations", page 110
✓ "Workflow des plans d'action", page 113

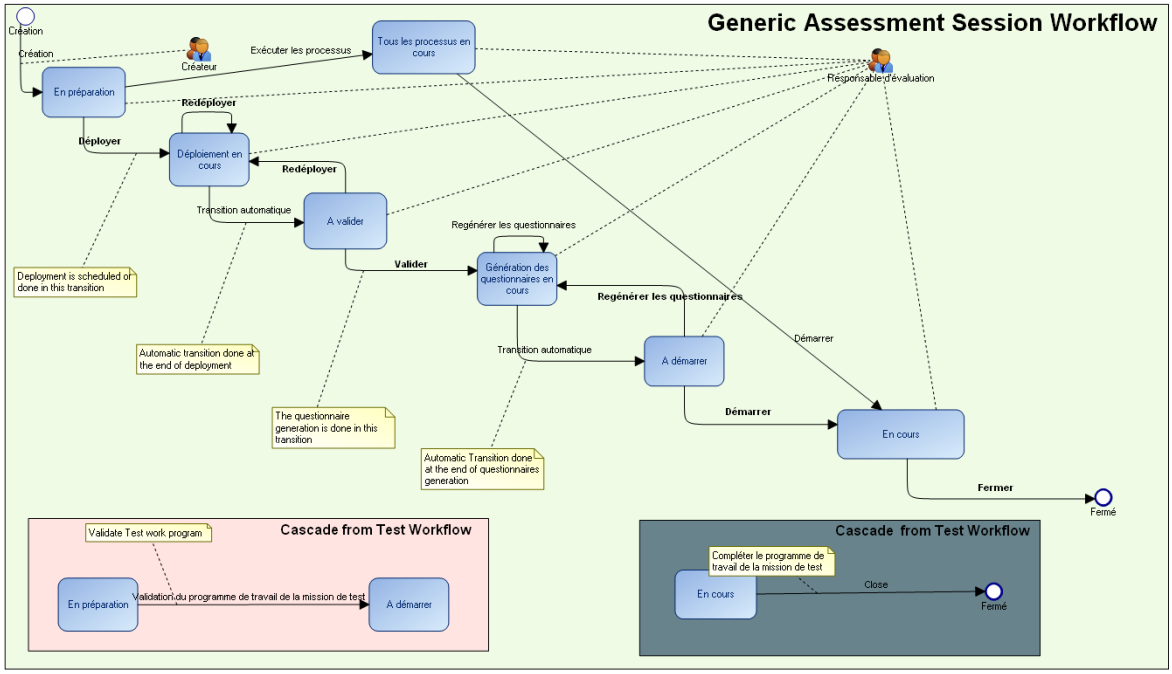
WORKFLOW DES ÉVALUATIONS

☛ *Pour un exemple d'enchaînement possible de workflow avec campagne, voir "Lancer une campagne et ses sessions d'évaluation", page 53.*

Workflow générique d'une campagne d'évaluation



Workflow générique d'une session d'évaluation



Workflow générique des questionnaires

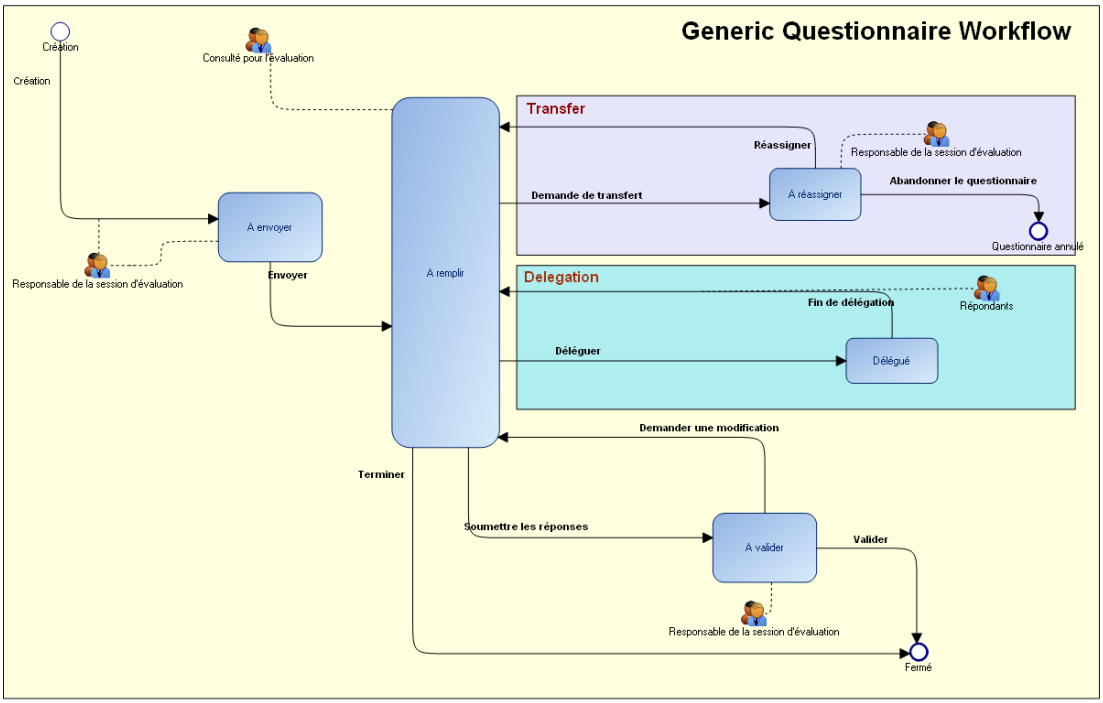
Les questionnaires sont reliés à une session d'évaluation et contiennent une ou plusieurs questions.

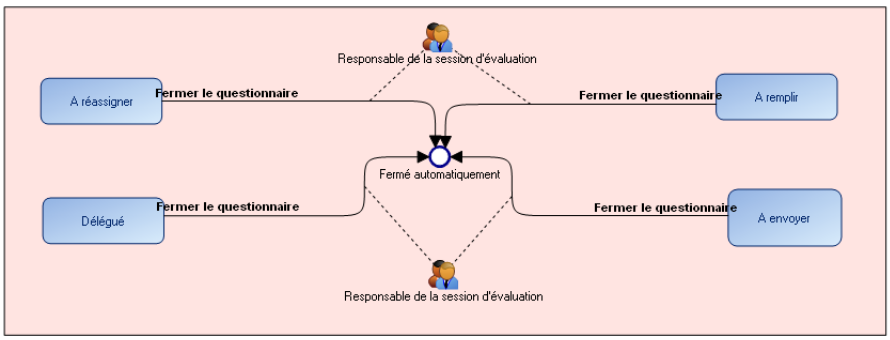
Les questionnaires sont générés en fonction du périmètre défini dans la session d'évaluation, du modèle d'évaluation ainsi que du questionnaire d'évaluation.

Ils sont envoyés automatiquement aux répondants lorsque la session d'évaluation démarre.

Un répondant peut transférer le questionnaire au responsable d'évaluation s'il n'est pas le destinataire approprié. Il peut également le déléguer à un autre répondant si tout ou partie du questionnaire peut être délégué.

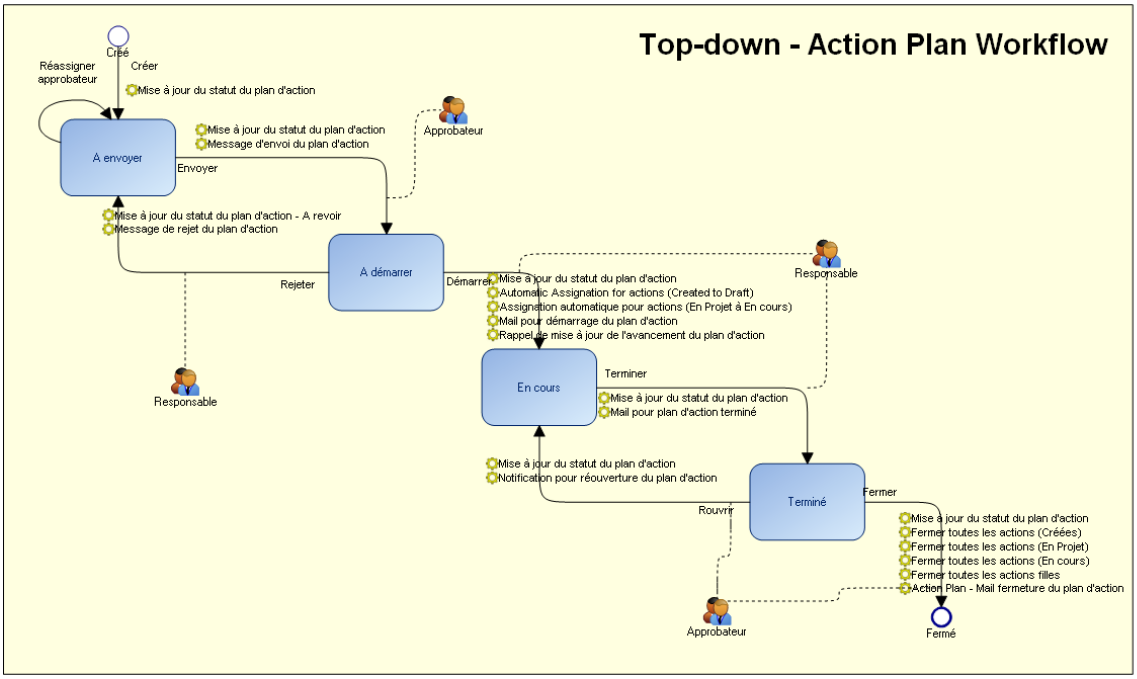
Le répondant ferme le questionnaire après l'avoir rempli si le workflow ne prévoit pas de validation. Il peut également l'envoyer pour validation au responsable de la session.



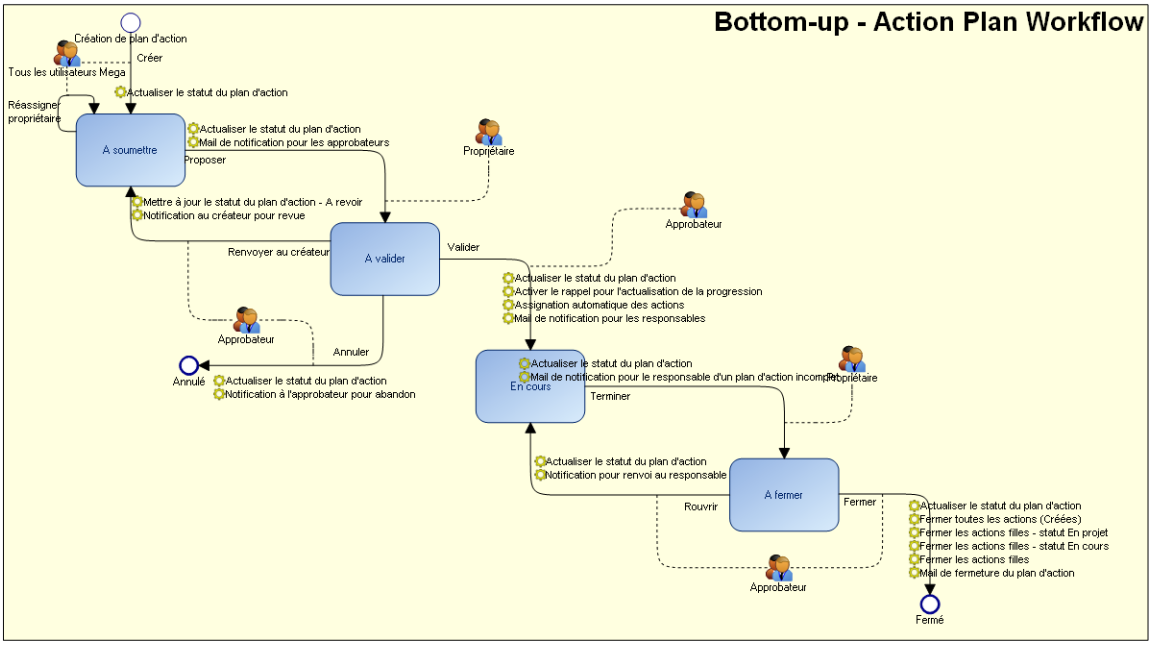


WORKFLOW DES PLANS D'ACTION

Workflow de plan d'action "top-down"



Workflow de plan d'action "bottom-up"



Workflow d'une action