****

**Guide méthodologique type de contrôle interne pour un OPH**



**décembre 2023**

Sommaire

[1. Introduction du directeur général ou du président 3](#_Toc62570192)

[1.1 Les enjeux du contrôle interne 3](#_Toc62570193)

[1.2 La gouvernance du contrôle interne 3](#_Toc62570194)

[1.3 Référentiels applicables 4](#_Toc62570195)

[1.4 La démarche de contrôle interne mise en œuvre 4](#_Toc62570196)

[1.5 Conclusion 4](#_Toc62570197)

[2. Enjeux et définitions du contrôle interne pour le secteur du logement locatif social 5](#_Toc62570198)

[2.1 Le contexte et les exigences réglementaires relatifs au contrôle interne 5](#_Toc62570199)

[2.2 Concepts clés et définitions 6](#_Toc62570200)

[2.3 Gestion globale des risques et contrôle interne 8](#_Toc62570201)

[2.4 Les 3 lignes de défense 9](#_Toc62570202)

[2.5 Coordination et interactions avec le contrôle de gestion 10](#_Toc62570203)

[2.6 Coordination et interactions avec les démarches qualité 11](#_Toc62570204)

[3. Les composantes du contrôle interne 11](#_Toc62570205)

[3.1 Environnement de contrôle 11](#_Toc62570206)

[3.2 Evaluation des risques 15](#_Toc62570207)

[3.3 Activités de contrôle 24](#_Toc62570208)

[3.4 Pilotage 25](#_Toc62570209)

[3.5 Information et communication 26](#_Toc62570210)

[4. Les acteurs 27](#_Toc62570211)

[4.1 La filière hiérarchique 27](#_Toc62570212)

[4.2 La filière fonctionnelle 28](#_Toc62570213)

[5. Le déploiement du contrôle interne et son manuel 29](#_Toc62570214)

[5.1 Organigramme fonctionnel nominatif 29](#_Toc62570215)

[5.2 Habilitations dans les systèmes d’information 30](#_Toc62570216)

[5.3 Logigramme 30](#_Toc62570217)

[5.4 Procédure détaillée 32](#_Toc62570218)

[5.5 Plan de contrôles 32](#_Toc62570219)

[5.6 Documentation 33](#_Toc62570220)

Ce guide a été établi dans le cadre de la démarche d’appui auprès des OPH initiée par la Fédération accompagnée par Grant Thornton. Il s’agit de la version au 7 décembre 2023.

* 25 mai 2021 : première édition
* 7 décembre 2023 : mise à jour des liens internet

1. Introduction du directeur général ou du président

Le présent guide vise à présenter, tant en interne, qu’en externe, la démarche de contrôle interne à mettre en place par l’Office. Il est de bonne pratique que ce guide soit introduit par la direction générale, à la fois car c’est elle qui est responsable in fine de la bonne maîtrise des risques mais aussi pour montrer l’engagement de la direction sur ce sujet et montrer la voie à l’ensemble des collaborateurs.

Vous trouverez ci-joint les thèmes qui nous semblent devoir être abordés et une proposition de rédaction qui devra être appropriée par l’office et adaptée autant que de besoin.

Cette introduction peut s’articuler autour des thématiques suivantes et ne doit pas excéder une à deux pages.

* 1. Les enjeux du contrôle interne

Ce premier chapitre permet de présenter les finalités du contrôle interne pour votre office, les principaux objectifs que vous lui assignez et permet de faire le lien avec d’autres démarches existantes, à titre d’exemple citons des engagements éthiques, sociaux ou sociétaux. Il permet aussi de commencer à mobiliser l’ensemble des acteurs internes qui d’une manière ou d’une autre y contribueront.

**Exemple de rédaction :**

« Le Contrôle Interne au sein de *« nom de l’office »,* vise à assurer que :

* la réalisation de ses objectifs s’effectue en conformité avec les lois et réglementations en vigueur, les principes déontologiques de « nom de l’office » ;
* les orientations fixées par le conseil d’administration sont mises en œuvre ;
* les actifs et la réputation de *« nom de l’office »* sont protégés ;
* les informations financières et comptables sont fiables et élaborées avec sincérité.

L’atteinte de ces objectifs ne pourra se faire que collectivement. Le contrôle interne est l’affaire de tous, de l’ensemble des collaborateurs de l’office, sa direction et son conseil d’administration.

Cet engagement prend racine dans une culture de rigueur et de service qui caractérise notre office, supporté par l’ensemble de l’équipe de direction ainsi que par le conseil d’administration. »

* 1. La gouvernance du contrôle interne

Ce chapitre expose l’organisation que vous allez mettre en place pour supporter la démarche de contrôle interne, le rôle des différents acteurs.

**Exemple de rédaction :**

« La volonté de mettre en place un dispositif de contrôle interne efficace au sein de « nom de l’office » trouve son origine dans le souci du conseil d’administration d’avoir une organisation la plus efficace possible au service de l’ensemble de nos missions et de satisfaire au mieux nos locataires. Le directeur général met en œuvre ce dispositif, en pilote les résultats et s’assure de son efficacité dans la durée. Pour ce faire, il s’appuie sur un responsable du contrôle interne, garant de la méthodologie et du suivi opérationnel de son fonctionnement et de pilotes de contrôle interne dans les directions qui déploient et mettent en œuvre au quotidien le contrôle interne. »

* 1. Référentiels applicables

Ce chapitre permet de faire le lien entre votre démarche et la cohérence de cette dernière avec les meilleurs référentiels connus en la matière. Vis-à-vis des équipes internes ou des contrôleurs externes, ces références sont un gage de qualité.

**Exemple de rédaction :**

« Le présent guide de contrôle interne décrit la méthodologie et les outils utilisés par l’office pour mettre en œuvre son contrôle interne. Pour ce faire, nous nous sommes appuyés sur les outils et les méthodologies développés par un certain nombre d’acteurs experts de ce domaine dont :

* COSO : Committee Of Sponsoring Organization, <https://www.coso.org/guidance-on-ic>
* IFACI : Institut Français de l’Audit et du Contrôle Interne, <https://www.ifaci.com>
* AMRAE : Association pour le Management des Risques et des Assurances de l’Entreprise, <https://www.amrae.fr>
* FERMA : Federation of European Risk Management Associations. » <https://www.ferma.eu>
  1. La démarche de contrôle interne mise en œuvre

Ce chapitre explique brièvement comment votre contrôle interne a été structuré et montre pour un lecteur avisé que cette structuration est cohérente avec les référentiels cités ci-avant.

**Exemple de rédaction :**

« Le contrôle interne de « nom de l’office » est structuré autour de nos processus métier et support, à partir desquels une analyse et une hiérarchisation des risques a été effectuée. Face à ces risques, « nom de l’office » a déployé une organisation et un système d’information pour les maîtriser.

Ce dispositif fait l’objet de contrôles annuels pour s’assurer de son bon fonctionnement. Les résultats de ces contrôles sont présentés à la direction générale qui prend les mesures nécessaires pour améliorer en permanence ce dispositif. »

* 1. Conclusion

Ce dernier chapitre a une dimension plus managériale et vise à faire s’approprier et faire prendre conscience aux équipes que cette démarche ne pourra pas prendre corps sans eux et sans leur contribution active à sa construction puis à son déploiement au quotidien.

**Exemple de rédaction :**

« Nous comptons sur l’implication de toutes et tous dans cette démarche, qui passe par une vision partagée de nos risques et un souci commun de les maîtriser. Cette démarche fait partie des actions importantes qui sont mises en œuvre et qui contribuent à l’atteinte et à la réussite de nos ambitions stratégiques. »

1. Enjeux et définitions du contrôle interne pour le secteur du logement locatif social
   1. Le contexte et les exigences réglementaires relatifs au contrôle interne

Le contrôle interne concerne toutes les organisations, qu’elles soient publiques ou privées et le secteur du logement social n’y déroge pas.

Nos missions, notre engagement dans la société, notre poids économique, nos enjeux politiques font que le secteur du logement locatif social doit se donner les moyens et les outils pour maîtriser les risques liés à ses activités et démontrer la pertinence de son organisation et l’efficience de sa gestion.

La loi ELAN entraîne une restructuration profonde du secteur, avec une volonté de le rendre plus performant. Elle définit la notion de groupe OLS, qu’il soit capitalistique ou non (société de coordination). Ces groupes ont une liberté de choix stratégique et des obligations communes, particulièrement :

* cadre stratégique patrimonial commun s’appuyant sur le plan stratégique de patrimoine de chaque organisme,
* cadre stratégique d’utilité sociale,
* politique technique, politique d'achat des biens et services, unité identitaire.

Ces obligations communes contraignent les acteurs de ce secteur à repenser leur organisation. Par ailleurs, l’instauration de la réduction du loyer de solidarité inclue à la loi de Finances 2018 a entraîné une baisse des ressources, donc une exigence de pilotage accrue.

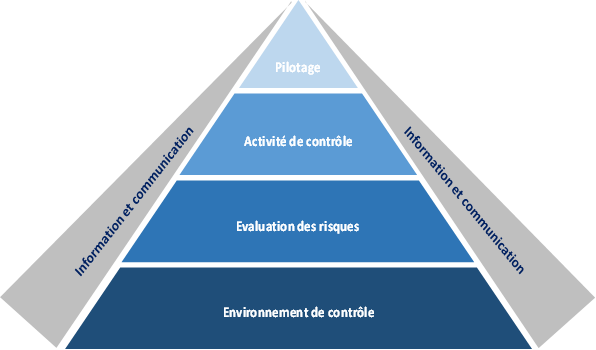
Enfin, un cadre réglementaire, de plus en plus évolutif, se caractérise, par :

* la loi sur la transparence, la lutte contre la corruption et la modernisation de la vie économique, dite « Sapin 2 »,
* les obligations en matière de protection des données (loi Informatique et Libertés de 2018 transposant la directive européenne relative au Règlement Général de Protection des Données),
* la comptabilité commerciale obligatoire pour tous les OPH,
* les attentes exprimées par les corps de contrôle (notamment Agence Nationale de Contrôle du Logement Social , dite ANCOLS, et les Chambres Régionales des Comptes), pour mémoire, la mission de contrôle de l’Agence recouvre, outre la vérification du respect de la législation et de la réglementation, l’évaluation des procédures de contrôle interne et d'audit interne mises en place par les organismes.[[1]](#footnote-1) Les attentes de ces corps de contrôle impliquent une maîtrise des risques et la mise en place d’un contrôle interne de qualité qui puisse traiter de l’ensemble des risques des offices.
  1. Concepts clés et définitions

La définition du contrôle interne retenue pour la rédaction de ce guide est conforme au référentiel COSO (Committee Of Sponsoring Organizations of the Treadway Commission), référentiel le plus largement utilisé dans la mise en place de dispositifs de contrôle interne :

« Le contrôle interne est un processus mis en œuvre par le conseil d'administration, le management et les collaborateurs d'une entité, destiné à fournir une assurance raisonnable quant à la réalisation d’objectifs liés aux opérations, au reporting et à la conformité. »

Afin de déployer un dispositif de contrôle interne efficient, le COSO préconise de travailler sur 5 composantes complémentaires au sein de l’organisation.

Figure 1 : Pyramide du COSO (Committee Of Sponsoring Organisation of the tradeway commission)

La notion de risque est fondamentale dans la démarche de contrôle interne, car c’est autour des risques que va se construire le dispositif de contrôle interne.

Un risque peut se définir comme un évènement susceptible d’empêcher l’atteinte des objectifs du processus ou de l’organisation. Cet évènement peut être potentiel (ne s’être jamais produit) ou avéré (l’entité a déjà fait face au risque). Exemples de risques :

* ne pas être en conformité avec la réglementation en vigueur concernant la sécurité des personnes et du patrimoine : entretien annuel périodique des chaudières individuelles et à gaz (incendie), sécurisation des ascenseurs, accident majeur du personnel (MO), etc.,
* quittancement inexact (défaut d’évaluation des surfaces, baux séparés pour les emplacements de stationnement),
* dégradation du niveau des créances locataires non recouvrées,
* non-respect de la commande publique : passation des marchés (défaut de publicité ou de mise en concurrence notamment), computation des seuils et dysfonctionnement dans l’exécution des marchés,
* non-respect d’obligations réglementaires (contingent préfectoral non identifié lors des attributions, enregistrement et radiation de la demande, droit au maintien dans les lieux des locataires non suivi, dépassement de plafond de loyers convention APL, enregistrement sur 18 positions NUD (numéro unique départemental) dans l’infocentre du Système National d’Enregistrement dit SNE…).

Le contrôle interne est imbriqué dans l’organisation et donc complètement intégré dans la conduite des activités de chacun. Il fait partie intégrante du processus.

Le contrôle interne est « universel » et concerne toutes les dimensions de la gestion d’une organisation (pas uniquement les aspects financiers & comptables). Tous les personnels de « nom de l’office » quel que soit leur statut contribuent à l’efficacité du contrôle interne (responsables et collaborateurs).

**En synthèse :**



* 1. Gestion globale des risques et contrôle interne

L’utilisation de certains termes peut porter à confusion, aussi il nous semble nécessaire de bien distinguer ce que l’on entend par la gestion des risques dits opérationnels (contrôle interne) et par la notion de gestion globale des risques.

Une partie de la distinction entre la gestion des risques opérationnels (contrôle interne, référentiel COSO) et la gestion globale des risques (référentiel COSO 2) tient au périmètre des risques couverts.

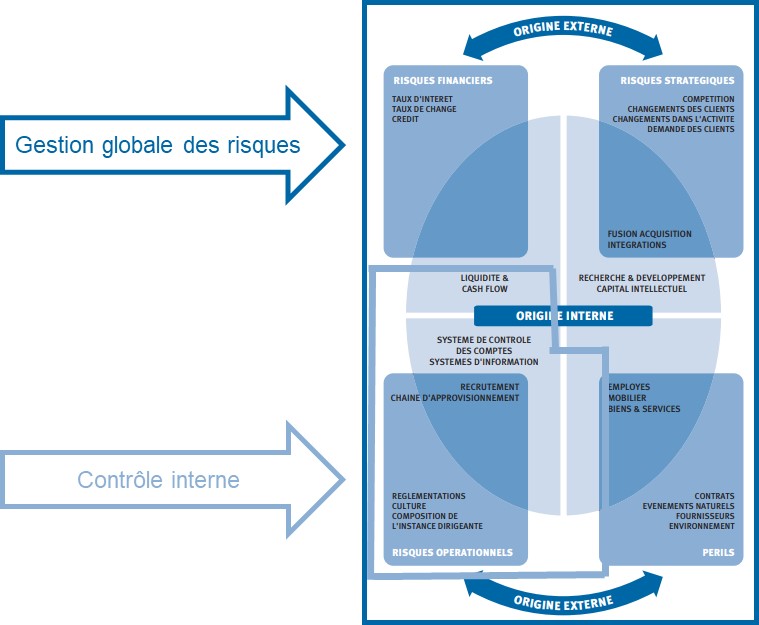
Le contrôle interne se focalise sur les risques dits opérationnels, c’est-à-dire l’ensemble des risques portés par les processus, par l’organisation, l’ensemble des risques auxquels « nom de l’office » peut être confronté dans ses activités au quotidien.

Malheureusement, ce ne sont pas les seuls risques auxquels les offices sont confrontés, car ils font aussi face à des risques plus globaux, plus transversaux qui peuvent fragiliser le modèle économique et social de l’office, remettre en cause certaines de ses activités.

La gestion globale des risques intègre à la fois les risques opérationnels mais élargit la gestion a d’autres risques également afin de donner une vision holistique de l’ensemble des menaces auxquelles est soumis « nom de l’office ».

Il s’agit ainsi de deux démarches complémentaires qui donnent à la direction une vision globale de ses risques et lui permet de mettre en place des plans de remédiation adaptés. Cette complémentarité est illustrée dans le schéma ci-contre en partant de l’univers des familles de risques définis par le « cadre de référence de la gestion des risques » publié par la fédération européenne des associations de gestion des risques (FERMA).

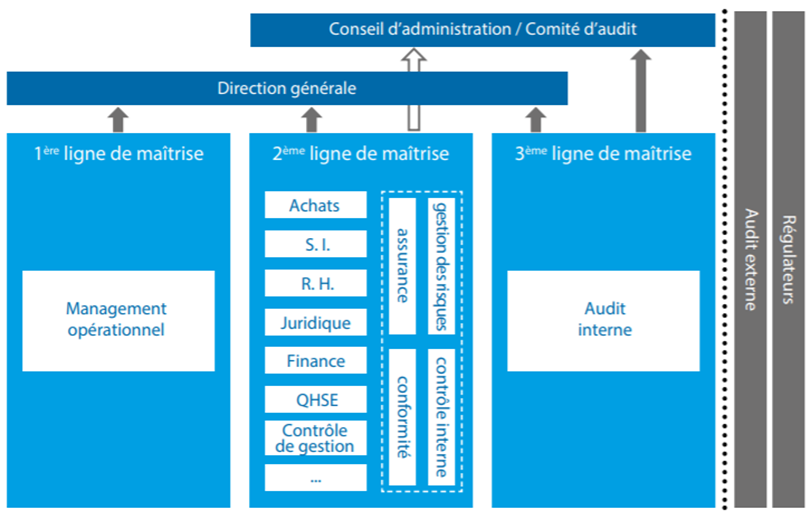
Figure  : Cadre de référence de la gestion des risques – FERMA (Federation of European Risk Management Associations)



* 1. Les 3 lignes de défense

Le contrôle interne fait partie intégrante du système de gestion des risques et est clairement positionné comme un dispositif de 2nd niveau, conformément aux pratiques de place, qui sont traduites dans la prise de position de l’IFACI (Institut Français de l’Audit et du Contrôle Interne) et de l’AMRAE (Association pour le Management des Risques et des Assurances de l’Entreprise), concernant les trois lignes de maîtrise des risques des entreprises.

Les trois lignes de défense ou dites de « maîtrise » sont distinctes mais complémentaires, et agissent conjointement face aux risques.

Figure  : les lignes de maîtrise

Source : Adapter l’organisation de l’entreprise pour une gestion efficiente des risques et des opportunités - IFACI

La première ligne de maîtrise est constituée par les responsables opérationnels et leurs équipes. Les responsables opérationnels ont en charge de mettre en œuvre un dispositif de contrôle adéquat sur les processus dont ils ont la responsabilité afin d’évaluer et diminuer les risques.

La deuxième ligne de maîtrise est constituée :

* des différentes fonctions transversales qui élaborent des procédures et des modes opératoires (achats, ressources humaines, système d’information, qualité, …),
* des fonctions dédiées à l’animation du dispositif global de maîtrise des risques, dont fait partie le contrôle interne.

Ce deuxième niveau de maîtrise des risques doit permettre la structuration et la maintenance du dispositif de maîtrise des activités notamment en assistant les opérationnels dans l’identification des risques, l’exécution des contrôles et la communication du niveau de maîtrise des activités.

La troisième ligne de maîtrise est constituée par une fonction d’audit interne indépendante souvent rattachée au plus haut niveau de l’organisation. La fonction d’audit interne a pour objectif de donner une assurance raisonnable sur le niveau de maîtrise des activités aux instances de gouvernance dont la direction générale de l’office, selon une approche fondée sur le risque.

Le contrôle externe peut être exercé par le commissaire aux comptes. Dans ce cas, il ne concerne que « des procédures de contrôle interne et de gestion des risques qui sont relatives à l'élaboration et au traitement de l'information comptable et financière » (cf. Normes Exercice Professionnel 9505).

L’évaluation du contrôle interne par le régulateur va, lui, concerner l’ensemble du périmètre de l’entité.

Le commissaire aux comptes peut aussi être sollicité dans le cadre de ses prestations annexes pour un audit du processus informatique sur la qualité et la sécurité des données.

* 1. Coordination et interactions avec le contrôle de gestion

La fonction de contrôle interne est coordonnée aux autres fonctions d’amélioration des performances de l’organisation et notamment le contrôle de gestion ou encore la qualité, qui sont aussi des fonctions qui composent la deuxième ligne de défense. Toutefois, ces deux fonctions ne sont pas redondantes avec le contrôle interne mais complémentaires et interagissent entre elles.

Notamment, il semble nécessaire de bien définir les rôles respectifs du contrôle interne et du contrôle de gestion. La distinction entre le contrôle interne et la qualité est abordée plus loin.

Chacun a un périmètre et des responsabilités clairement définies et complémentaires :

* le contrôle de gestion a pour mission de s’assurer de l’adéquation entre les actions et les projets de l’entreprise avec la stratégie définie. Il consiste avec l’aide d’un logiciel décisionnel à restituer, au travers de tableaux de bord mensuels et d’analyses détaillées, le suivi de l'évolution d’indicateurs (des produits et des dépenses de fonctionnement et d'investissement, de la qualité de service, de la performance des prestataires) ainsi que l’élaboration et le suivi du budget. Le contrôle de gestion éclaire la direction sur la réalité et l’effectivité de la mise en œuvre de la stratégie et des orientations fixées par elle.
* Le contrôle interne s’assure que l’organisation qui a été définie permet de maîtriser les risques opérationnels inhérents à l’organisation existante et que cette organisation est pertinente pour atteindre les objectifs définis par la direction.

Le contrôle de gestion s’assure donc que la stratégie est mise en œuvre et produit les résultats escomptés là où le contrôle interne s’assure que l’environnement de contrôle, l’organisation, les processus sont sécurisés et que l’organisation est efficiente pour servir la stratégie. La conjonction de ces deux fonctions permet de s’assurer que l’organisation mise en place pour servir la stratégie s’inscrit dans un environnement de contrôle maitrisé et que cette organisation donne les résultats escomptés.

Par ailleurs, leurs missions respectives servent les intérêts de chacune :

* le contrôle interne joue un rôle essentiel dans la qualité des données de gestion, comptables et financières dont se sert le contrôle de gestion pour faire ses analyses. Il est rattaché à la direction générale.
* Le contrôle de gestion par ses analyses et sa connaissance des métiers et des organisations permet de détecter des anomalies ou des facteurs de risques qui permettent d’alimenter la dynamique d’amélioration continue du contrôle interne. Il est en général une composante de la direction administrative et financière.

Il s’agit de fonctions clairement définies, qui se complètent.

*(Nota : Selon la taille des offices, la personne qui les porte pourrait être la même si la fiche de poste distingue bien les deux fonctions).*

* 1. Coordination et interactions avec les démarches qualité

La démarche qualité de type ISO 9001 V2015 et le contrôle interne partagent une approche commune qui part des processus de fonctionnement de la structure et d’une analyse des risques qui porte sur ces processus. Ces deux démarches reposent sur un principe commun d’amélioration continue à partir de contrôles et d’un système de pilotage.

En revanche, ces deux démarches n’interviennent pas sur le même périmètre. Le contrôle interne intègre l’ensemble des risques de l’organisation, là où la qualité se focalise sur une typologie de risques plus restreinte, orientée vers la satisfaction client et la qualité des services et des prestations rendues. Ces deux démarches divergent enfin dans leur finalité. La démarche qualité, opposable aux tiers, répond à une norme certifiante qui est vérifiée par un tiers externe, là où le contrôle interne est une démarche de management interne qui ne fait pas l’objet d’une certification par un tiers externe.

*(Nota : Un office qui aurait déjà mis en place une démarche qualité pourrait se servir du système de management qui porte cette démarche pour y intégrer le contrôle interne, en créant ainsi un système de management intégré qualité et contrôle interne. Le responsable qualité pourrait aussi devenir le responsable du contrôle interne).*

1. Les composantes du contrôle interne

**19**

Comme évoqué précédemment à la section 2, le COSO indique qu’il convient de travailler sur 5 composantes pour déployer un dispositif de contrôle interne.

Cette partie a pour vocation de présenter les outils clés qu’il convient de construire, afin de s’assurer du caractère opérationnel du dispositif de contrôle interne au sein de l’office.

Figure  : la pyramide du COSO



* 1. Environnement de contrôle

L’environnement de contrôle est l’environnement dans lequel les personnes accomplissent leurs tâches et assument leurs responsabilités. Il intègre notamment la compétence individuelle des collaborateurs et surtout leur intégrité, leur déontologie et leurs expertises. L’environnement de contrôle constitue le socle de toute organisation.

Au-delà de la culture de l’entreprise (mode de management et de supervision, responsabilité sociale et environnementale, implication de la direction…), l’environnement de contrôle repose sur trois leviers :la documentation, l’organisation et la traçabilité.

* + 1. La documentation

Le levier « documentation » vise principalement à documenter l’organisation, les procédures, les contrôles et les risques.

Exemple de mesures : élaboration et diffusion d’un organigramme fonctionnel nominatif, d’une cartographie des processus et d’une cartographie des risques, d’une fiche de procédure et des contrôles associés, etc.

* + 1. L’organisation

Le levier « organisation » correspond à la définition et l’organisation des tâches, des acteurs et des contrôles.

Une organisation efficiente repose sur :

* le principe de séparation des fonctions,
* le système de délégations prévues pour les OPH à l’article R421-18 du CCH,
* un système d’information adapté servi par un système d’habilitations informatiques actualisé.

Le levier « organisation » vise à garantir le principe de continuité par une attribution claire des tâches de chaque acteur (titulaire/suppléant, séparation des tâches) et une gestion suivie de ces tâches. Les habilitations informatiques doivent en outre être conformes aux attributions de chacun.

Enfin, le levier « organisation » consiste à s’assurer que les contrôles sont correctement menés et ce sur l’ensemble du processus, depuis le service responsable de l’acte initial (ou du fait générateur) jusqu’au comptable. Ces contrôles peuvent être :

* réalisés par les opérationnels :
* auto-contrôles,
* contrôles mutuels : Contrôles exercés par un salarié/agent sur les opérations effectuées en amont par un autre salarié/agent (principe de séparation des tâches) ;
* «applicatifs» lorsqu’ils sont intégrés au SI :
* manuels i.e. le processus de validation par un responsable approprié,
* semi-automatisé ou automatisé i.e. la vérification que l’enregistrement sollicité est conforme aux prescriptions définies dans les paramètres du SI.

Les contrôles applicatifs semi-automatisés ou automatisés doivent être privilégiés cas ils permettent de générer une alerte ayant pour objectif d’informer l’utilisateur du résultat du contrôle ou être bloquants, empêchant ainsi l’utilisateur d’aller plus loin si le résultat du contrôle est négatif.

* + 1. La traçabilité

Le levier « traçabilité » a pour objectif de permettre à tout moment de justifier une opération, en remontant de l’enregistrement en comptabilité jusqu’au fait générateur de l’opération et inversement.

Exemple : modification du système d’information afin de tracer l’intervention des acteurs, mise en place d’interface entre des applications informatiques pour éviter les ruptures applicatives, gestion des habilitations informatiques et des mots de passe, archivage des pièces justificatives, etc.

En pratique, la traçabilité des acteurs et des opérations comptables est de plus en plus fréquemment portée par les systèmes d’information (sous réserve du respect du dispositif d’habilitations, du caractère individuel des identifiants et du secret des mots de passe).

L’environnement de contrôle se construit usuellement via une approche processus permettant d’avoir une vision globale et transversale de l’entité et de l’exhaustivité des activités de celle-ci.

Pour se faire une cartographie des processus de l’office doit être établie.

* + 1. Proposition de cartographie type des processus d’un office

**Processus de Management**

1. **Gouvernance de l’office**

* Pilotage et organisation
* Communication
* Conformité
* Déclarations sectorielles (Harmonia, RPLS, OPS, SNE, etc…)

**Processus opérationnels**

**Patrimoine**

1. **Développement du patrimoine**

* Acquisition du foncier
* Assistance à maîtrise d’ouvrage (conception, réalisation, livraison de l’ouvrage)
* Gestion des garanties : parfait achèvement, biennale, décennale, dommage ouvrage
* Aménagement pour le compte de collectivité territoriale et lotissement
* Construction d’équipements pour des tiers (Collège, restaurant CROUS, etc…)

1. **Réhabilitations**

* Energétique
* Opération ANRU

1. **Maintenance et entretien**

* Maintenance du bâti et des installations
* Sécurité, mise aux normes
* Gestion des sinistres

1. **Vente du patrimoine**

* Cession de patrimoine locatif social (vente à personnes physiques et vente en bloc)
* Accession sociale à la propriété
* Commercialisation de logements neufs (VEFA inversée)

**Gestion locative**

1. **Gestion locative personnes physiques**

* Entrée et sortie du locataire
* Assurance habitation
* Gestion des réclamations
* Concertation locative

1. **Attribution des logements et parcours résidentiel**

* Gestion des attributions (CALEOL)
* Attributions aux publics prioritaires
* Mutations internes
* Droit au maintien dans les lieux

1. **Quittancement et créances locatives**

* Recouvrement
* Gestion du contentieux

1. **Gestion locative des personnes morales**

* Gestion globale au profit de personnels particuliers (L 422-2 CCH : gendarmerie, police nationale, S. incendie et secours, …)
* Résidences autonomie et habitat spécialisé (foyers, EHPAD)
* Locaux d’activité

1. **Syndics de copropriétés**
2. **Tranquillité résidentielle**
3. **Prestations de service diverses**

* Parkings
* Conciergerie
* Vente d’électricité

**Processus Supports**

1. **Suivi financier et budgétaire**
2. **Comptables et financiers**

* Achats
* Capitaux propres
* Provisions pour risques et charges
* Etats Impôts
* Immobilisations et stocks
* Recettes et créances
* Ressources humaines
* Trésorerie

1. **Ressources humaines**
2. **Achats**

* Achats d’un montant inférieur au 1er seuil[[2]](#footnote-2) de passation des marchés
* Achats d’un montant supérieur au 1er seuil

1. **Système d’information**

* Documentation générale, architecture
* Habilitations
* Mécanismes d’authentification
* Traçabilité des opérations
* Gestion des incidents
* Procédures de sauvegardes et de restauration
* Politique de sécurité du système d’information
* Plan de reprise d’activité

1. **Moyens généraux**

* Pools de véhicules
* Matériel général
* Siège social et directions territoriales
  1. Evaluation des risques
     1. L’univers des risques

L’univers des risques représente les grandes familles de risques auxquels l’office peut se trouver confronté, il permet ainsi de compléter la vision des risques par processus par une vision des risques par nature.

L’univers des risques est aussi le point d’articulation, de mise en cohérence des différentes cartographies que l’office peut être amené à réaliser : cartographie de contrôle interne, cartographie globale de la direction générale, cartographie des risques pénaux des dirigeants, cartographie Sapin II, cartographie des risques des systèmes d’information….

Ces cartographies ne peuvent pas se consolider au sein d’une seule pour des raisons évidentes de lisibilité, d’interprétation et d’utilisation des résultats. En revanche l’univers des risques offre à la direction une vision transversale sur les familles de risques.

Figure 5 : Articulation des différentes cartographies autour de l’univers des risques

La structuration de l’univers des risques repose sur les 4 grandes familles de risques définies dans le référentiel de gestion des risques proposé par FERMA.

Figure  : Univers des risques

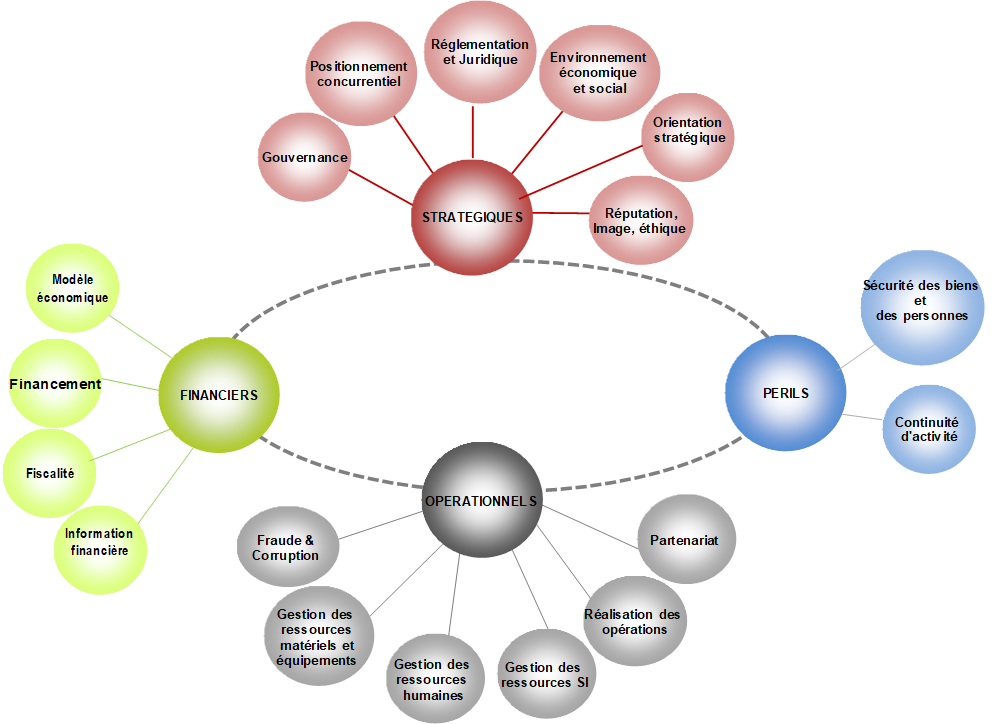


Tableau  : Description des risques stratégiques

|  |  |  |
| --- | --- | --- |
| Niveau 1 | Niveau 2 | Exemples / illustrations (non exhaustives) |
| Stratégiques | Gouvernance | Risques liés à un mode de gouvernance mal défini (ex : conflits d’intérêt, relation avec les élus des collectivités territoriales/EPCI, système de délégations, présence d’un comité d’audit, prise de participation, notamment au sein d’une Société de Coordination…)  Risques liés à la non-identification et présentation des conventions réglementées (transaction, baux conclus avec les membres du personnel) |
| Positionnement « concurrentiel » | Risques liés à un décalage entre l'offre et le marché, que ce soit en termes de produits ou de services  Positionnement concurrentiel face aux autres organismes de logement social, SEM de logements sociaux, sociétés HLM  Risques liés à la concurrence : émergence d'un nouvel acteur, agressivité de la concurrence  Risques liés aux nouveaux métiers et services offerts |
| Réglementation et juridique | Risques liés aux actions de la tutelle de l’Etat : contrôles, pratiques, recommandations, capacité à se conformer aux réglementations, remise en cause réglementaire de l’activité…  Risques liés aux contrats/conventions/licences/actes notariés  Risques liés aux problématiques de Propriété intellectuelle / Droit à l’image  Risques liés à la non-protection des données / CNIL / vie privée  Risques liés à la responsabilité civile ou pénale, système de délégations |
| Environnement économique et social | Risques liés à l’environnement économique, politique, social du secteur et aux changements de cet environnement |
| Orientation stratégique | Risques liés aux enjeux politiques de territoire, à la non prise en compte des innovations et des nouveaux acteurs  Pertinence des orientations stratégiques face au marché et à ses besoins, adaptation de l’offre locative à la demande, résorption de la vacance |
| Réputation, image, éthique | Risques liés à tout évènement qui pourrait nuire à la réputation de l’entité, à son image, au non-respect de ses valeurs, communication sur les réseaux sociaux |

Tableau  : Description des risques financiers

|  |  |  |
| --- | --- | --- |
| Niveau 1 | Niveau 2 | Exemples / illustrations (non exhaustives) |
| Financiers | Modèle économique | Risques liés à la gestion de la trésorerie, des conditions financières et du Besoin en Fonds de Roulement  Équilibre à long terme du modèle économique et de la viabilité |
| Financement | Risques liés au niveau d’endettement, à l’accès aux financements et/ou aux crédits Risques liés à l’accroissement du poids de la dette  Risques liés aux nouveaux modes de financement : titres participatifs |
| Fiscalité | Risques liés aux choix fiscaux |
| Information financière | Risques liés à la qualité de l’information financière, la qualité comptable, la certification des comptes |

Tableau  : Description des risques opérationnels

| Niveau 1 | Niveau 2 | Exemples / illustrations (non exhaustives) |
| --- | --- | --- |
| Opérationnels | Fraude / Corruption | Risques liés à toute forme de fraude ou malversation réalisée par un membre du personnel de l’office  Risques de détournement de fonds, de corruption active ou passive… Risques liés à toute forme de fraude ou malversation réalisée par un tiers de « nom de l’office » qu'il s'agisse d'un client, d'un bénéficiaire ou d'un partenaire.  Fraude au Président  Utilisation de l’IBAN de l’office par des locataires |
| Ressources matérielles et équipements | Risques liés aux défaillances des équipements (ascenseur, climatisation, chauffage…) et systèmes et/ou lié à un non-respect des délais légaux, réglementaires ou contractuels, panne, maintenance, maintien en condition opérationnelle  Risques liés à l’amiante, au plomb (absence constat de risque d'exposition au plomb (CREP, DAPP) Risques liés à l’indisponibilité du matériel Risques liés à la sécurité et la conformité des équipements de travail |
| Gestion des ressources humaines | Risques liés au processus RH (Compétences /Connaissances / Personnes clefs/ Recrutement /absences/contentieux/ Paie)  Risques liés aux Mouvements sociaux et syndicaux / Risques liés aux problématiques santé au travail (Risques psycho-sociaux, Qualité de vie au travail)  Non-respect de la durée légale du temps de travail  Document unique d’évaluation des risques professionnels (DUERP) Risques liés à l’intégrité des personnes (ex : accidents du travail, maladies professionnelles) |
| Gestion des ressources SI | Risques liés à la maintenance des équipements SI (Dysfonctionnement des infrastructures informatiques ; Indisponibilité totale ou partielle du système d'information Actes de malveillance (cyberattaque…) Système d’information insuffisamment développé et automatisé… |
| Réalisation des opérations | Risques liés au déroulement des processus en vigueur au sein de « nom de l’office », à l'exploitation des applications et logiciels ou progiciels et à leur fonctionnement  Risques de défaillance humaine dans la réalisation des opérations au cours d'un processus  Non-respect des procédures  Risques liés aux locataires / accédants/ clients (impayés, recouvrement, vieillissement de la population, paupérisation des locataires, troubles, …, non-respect des objectifs de mixité sociale sur le parc de logements / résidence) |
| Partenariat | Risques liés aux relations avec les collectivités territoriales / EPCI, les associations  Risques liés à la relation commerciale avec les fournisseurs (défaillance, carence, retard, malfaçon, réserves, retard…) |

Tableau  : Description des périls

|  |  |  |
| --- | --- | --- |
| Niveau 1 | Niveau 2 | Exemples / illustrations (non exhaustives) |
| Sécurité et Périls | Sécurité des personnes et des biens | Agressions Accidents (des locataires ou du personnel mais aussi les fournisseurs et sous-traitants) Actes de malveillance (dégradation de locaux…) Bâtiments et matériels non entretenus, dégradés…  Criminalité, incivilités, trafics, violences urbaines |
| Interruption d'activité | Crises majeures : catastrophes naturelles, incendie, attentats, pandémie, pollution, grève, conflits sociaux … |

* + 1. Cartographie des risques

L’analyse des risques est généralement formalisée au travers d’une cartographie des risques.

* Une cartographie des risques est :
* une représentation visuelle des risques de l’office, qui permet de repérer rapidement et facilement les risques à traiter en priorité,
* une identification, évaluation et hiérarchisation des risques des différents processus de l’office,
* le point de départ de tout le dispositif de contrôle interne.

Figure  : Diagramme temporel élaboration des cartographies



L’analyse de risques se décompose en 2 phases : l’identification et l’évaluation.

**Identification**

Pour identifier les risques, il convient de s’appuyer sur l’analyse des processus de l’office en veillant à:

* prendre en compte toutes les activités du processus et toutes les caractéristiques clés du processus (règlementation, systèmes d’information, niveau de compétences requis…),
* intégrer les éventuelles évolutions dans l’environnement externe ou interne de l’office, qui pourraient affecter l’atteinte des objectifs (évolutions réglementaires, changement de SI…).

**Évaluation**

Une fois les risques identifiés, il convient de les évaluer pour les hiérarchiser. Pour ce faire, il convient de définir des échelles de cotation pour évaluer les deux critères suivants :

* la probabilité de survenance : probabilité qu’un évènement non souhaité survienne (taux d’incidence),
* les impacts (financier, réputation, réglementaire et sécurité des personnes) : ensemble des conséquences engendrées par la survenance d’un évènement non souhaité.

***Risque brut = Probabilité \* Impact***

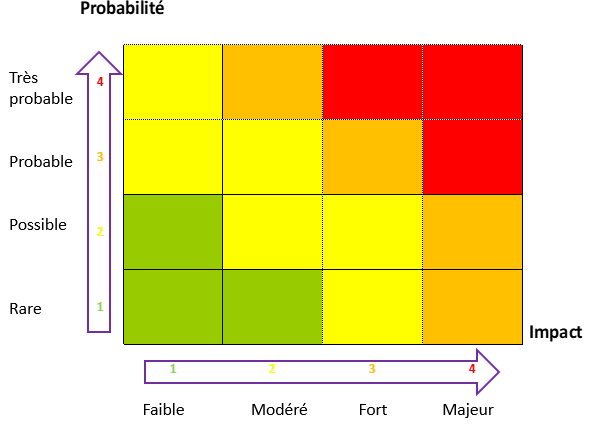
Tableau  : Exemple d’échelle pour la cotation de la probabilité

|  |  |  |
| --- | --- | --- |
|  | Probabilité | Description |
| 1 | Rare | Il est peu vraisemblable que le risque se réalise |
| 2 | Possible | Il est possible que le risque survienne |
| 3 | Probable | Il existe une possibilité sérieuse que le risque se réalise |
| 4 | Très probable | Le risque va vraisemblablement se réaliser |

Tableau  : Exemple d’échelle pour la cotation de l’impact

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Impact | Description | | | |
| **Financier** | **Image/ qualité de service** | **Juridique et réglementaire** | **Santé et sécurité des personnes** |
| 1 | Faible | Pas d’incidence visible sur le résultat et/ou le chiffre d'affaires | Visible en interne Aucun impact sur le niveau de satisfaction | Non-respect des directives opérationnelles (interne) | Impact faible sur la sécurité et la santé, pas d’arrêt de travail, pas de conséquences sur la vie quotidienne |
| 2 | Modéré | Impact visible sur le résultat et/ou le chiffre d'affaires mais sans remise en cause des équilibres financiers | Visible par peu de locataires / accédants/ clients/ prestataires sans conséquences néfastes | Non-respect des directives stratégiques (interne)  Sanctions administratives : URSSAF, FISC...  Constats d'irrégularité par l'ANCOLS, recommandations de la CRC… | Impact modéré pouvant entraîner des blessures légères ou un arrêt de travail court |
| 3 | Fort | Impact significatif sur le résultat et/ou le chiffre d'affaires nécessitant des mesures spécifiques | Visible par de nombreux locataires / accédants / clients/ prestataires avec conséquences néfastes | Sanction financière et/ou administrative du ministre chargé du logement à l'issue de contrôles diligentés par l'ANCOLS. Condamnations peu sévères par les juridictions (civiles/pénales/ administratives selon le cas) | Impact fort pouvant entraîner des blessures graves, conduire à une situation d’invalidité ou un arrêt de travail long |
| 4 | Majeur | Impact majeur sur le résultat et le chiffre d'affaires, remise en cause des équilibres financiers | Visible par un nombre significatif de locataires / accédants / clients / prestataires et/ou mise en cause de la structure dans le secteur d’activité : visible dans la presse spécialisée, par les publications des organes de contrôle | Proposition de retrait d’agrément. Condamnations sévères par les juridictions (civiles/pénales/ administratives selon le cas) | Impact majeur pouvant entraîner des conséquences irréversibles graves, voire le décès d’une personne |

Cette approche permet de déterminer, sur une matrice des risques bruts (qui est une représentation visuelle de l’analyse), le positionnement du risque selon son niveau de probabilité de survenance et son degré d’impact.

Figure  : Matrice des risques bruts

Le risque brut est le risque inhérent à toute activité. L’évaluation de ce risque via la probabilité de survenance et les impacts du risque brut se fait avant la prise en compte des éléments de maîtrise existant. Il s’agit donc d’évaluer le niveau de risque en faisant abstraction de ce qui permet aujourd’hui de le maîtriser.

La cartographie des risques bruts permet ainsi de hiérarchiser les risques les plus importants qui pèsent sur l’office.

Tableau  : Exemple de grille pouvant être utilisée pour évaluer les risques

Note de lecture : Score impact global brut : maximum des 4 notes données pour l’impact brut (financier, image/ qualité de service, réglementaire et juridique, santé et sécurité des personnes), Risque brut : produit matriciel du score de vraisemblance de l’impact brut et du score de l’impact global brut.

* 1. Activités de contrôle

Les activités de contrôle recouvrent l’ensemble des activités, procédures, contrôles, éléments d’organisation mis en œuvre par l’office pour maîtriser ses risques les plus importants.

Ces différents éléments de maîtrise sont recensés et évalués, afin d’en vérifier en permanence, la pertinence et l’efficacité, au regard des risques préalablement identifiés.

**Les dispositifs de maîtrise peuvent réduire les causes du risque, intervenir sur le risque lui-même ou limiter les conséquences du risque :**

* prévenir la survenance du risque,
* détecter la survenance du risque,
* protéger des conséquences du risque.

**Les dispositifs de maîtrise des risques opérationnels sont de différentes natures. Il peut s’agir :**

* d’éléments d’organisation :

organigramme / activité / mission, définition de fonctions (rôles et responsabilités), séparation des fonctions, habilitations (signatures, accès informatiques), gestion de l’adéquation charges / ressources / compétences, planification des travaux, traçabilité des informations.

* de la documentation :

réglementation, loi, procédures, modes opératoires, règles de gestion, guide utilisateur, supports de formation, notes de service, contrats de service.

* des contrôles automatiques :
* intégrés au SI : contrôles de saisie (blocage ou alerte), contrôle de cohérence des données (Traitements informatiques par lot (batch), rejets anomalies…),
* comme des comptes rendus de traitements (batch notamment), de rapprochements de systèmes (passage de comptabilité auxiliaire à comptabilité générale par ex.),
* de bonne fin d’exécution des traitements batch.
* Des contrôles humains :
* *a priori* : Auto-contrôle (avant et post saisie), validation...,
* *a posteriori*: contrôles par un autre acteur de l’activité (contrôle a posteriori, par sondage, sur échantillon…), contrôle hiérarchique, contrôle croisé…
* Des éléments de pilotage :
* existence d’objectifs et d’indicateurs quantitatifs (délais, nombre…) et qualitatifs (client, délais moyen, conformité…).

Une fois les éléments de maîtrise recensés, il convient d’évaluer leur efficacité au regard des risques. Comme pour les risques, cette évaluation doit être réalisée sur la base d’une échelle de cotation.

Tableau  : Exemple d’échelle pour les cotations des éléments de maîtrise

|  |  |
| --- | --- |
|  | Évaluation de la maîtrise  (Synthèse de l’efficacité des différents éléments de maîtrise) |
| 4 | Risque couvert par un dispositif de maîtrise adapté, formalisé, supervisé |
| 3 | Les éléments de maîtrise sont suffisants mais peuvent être améliorés dans la forme (formalisme, supervision …) |
| 2 | Les éléments de maîtrise sont insuffisants (pas assez nombreux) ou inadaptés (mal positionnés par rapport au risque) |
| 1 | Risques sans maîtrise ou maîtrise obsolète |

* 1. Pilotage

Le dispositif de contrôle interne est un ensemble d’outils contribuant :

* à l’amélioration continue de la maîtrise des activités,
* à la surveillance régulière des risques opérationnels.

L’ajustement et le pilotage du dispositif de contrôle interne peut être réalisé de façon pertinente au regard des résultats de l’évaluation des risques d’une part et de l’évaluation du dispositif de maîtrise existant d’autre part. L’adéquation entre ces deux niveaux d’évaluation peut se matérialiser sur la matrice ci-dessous.

Figure  : Matrice de priorisation des risques

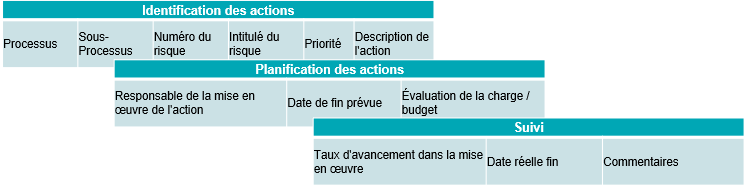
Le pilotage du dispositif de contrôle interne est un élément essentiel qui contribue à matérialiser sa valeur ajoutée. Il permet de prendre les bonnes décisions en fonction du niveau d’exposition aux risques de l’office.

**Les plans d’actions**

Il est nécessaire de mettre en place des actions face aux risques mis en exergue dans les zones de «risque critique». Un plan d’actions consiste notamment à :

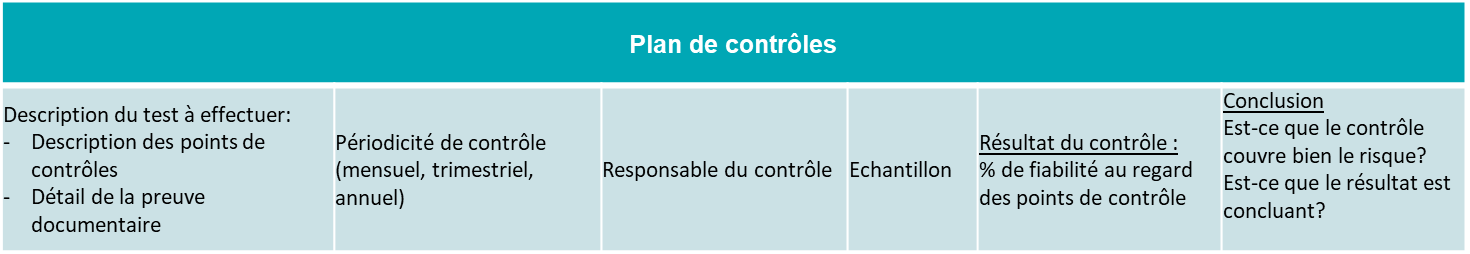
* améliorer et optimiser l’existant,
* créer et mettre en place de nouveaux éléments de maîtrise.

L’objectif de la mise en œuvre d’une nouvelle action de maîtrise sera de réduire le niveau « résiduel » constaté.

Figure  : Exemple de plans d’actions

**Les plans de contrôles**

La réalisation d’un plan de contrôles a pour objectif principal de vérifier la réalité et l’efficacité des éléments de maîtrise « clés » mis en place par rapport aux risques identifiés et qui constituent le 1er niveau de contrôle des activités. A cette fin, le plan de contrôles recense des contrôles de 2ème niveau, par exemple le contrôle d’un contrôle ou le contrôle d’un autre élément de maîtrise de 1er niveau : organisation, documentation, contrôle intégré au SI.

Figure  : Exemple de plan de contrôle

* 1. Information et communication

Les volets information et communication permettent de donner de la visibilité sur l’efficacité globale du dispositif de contrôle interne à travers le suivi d’indicateurs clés par exemple.

Ces informations permettent de communiquer vers les acteurs du dispositif, à la fois de manière ascendante (vers la direction générale ou le conseil d’administration) ou de manière descendante vers les opérationnels.

Ainsi, des indicateurs de suivi peuvent être mis en place, tels que des indicateurs de suivi du dispositif, des indicateurs quantitatifs et qualitatifs ou bien encore des indicateurs de mesure d’impact, permettant de donner de la visibilité sur la maîtrise des risques opérationnels.

1. Les acteurs

Comme cela a été évoqué au début de ce guide et dans la définition du contrôle interne, le contrôle interne est l’affaire de tous, du conseil d’administration, de la direction, en passant par le management intermédiaire jusqu’à l’ensemble des collaborateurs. Tous ont un rôle important à jouer mais tous n’ont pas le même rôle.

* 1. La filière hiérarchique
* **Le conseil d’administration**
* Il approuve les décisions stratégiques proposées par la Direction Générale.
* Il est informé annuellement des résultats du dispositif de contrôle interne et du niveau de maîtrise des risques de l’office.
* Il peut à tout moment interroger la direction générale sur la maîtrise des risques.
* **La direction générale**
* Elle propose au conseil d’administration les orientations et les objectifs généraux du contrôle interne, décide de l’organisation.
* Elle est « sponsor » du contrôle interne.
* Elle rappelle régulièrement les rôles et responsabilités de chacun au sein du dispositif de contrôle interne.
* Elle arbitre les plans d’actions proposés et suit leur réalisation.
* Elle analyse les résultats obtenus en termes de contrôle interne.
* Elle communique ces résultats au conseil d’administration.
* Elle valide la cartographie des risques.
* **Les directeurs et responsables hiérarchiques**
* Ils sont « sponsor » du contrôle interne au sein de leur direction.
* Ils contribuent à la sensibilisation de tous les acteurs à l’importance du contrôle interne, ils veillent au respect des procédures.
* Ils s’assurent du bon fonctionnement du dispositif de contrôle interne, de sa formalisation et de sa mise à jour régulière.
* Ils proposent au Directeur Général de valider la cartographie des risques opérationnels de leur domaine et s’assurent de sa mise à jour.
* Ils proposent au DG leurs plans d’actions correctifs et préventifs face à ces risques.
* Ils s’assurent de l’existence et du suivi des plans et des plans de contrôles.
* Ils suivent les résultats de ces contrôles et proposent au directeur général les conséquences sur l’organisation.
* Ils communiquent sur les résultats obtenus et sur les évolutions apportées à l’activité auprès de la direction générale en lien avec le responsable du contrôle interne.
* **Les correspondants contrôle interne**
* Ils sont la cheville ouvrière du contrôle interne dans les directions.
* Ils s’assurent de la mise à jour régulière de la documentation (processus, référentiel, procédure, cartographie, plans de contrôle) associée aux risques des processus.
* Ils mettent à jour régulièrement la cartographie des risques opérationnels de leur processus.
* Ils en tirent les conséquences en matière de plan d’actions de remédiation et d’évolution des plans de contrôle, qui seront proposés pour validation au directeur, puis au directeur général. Ils en suivent la mise en œuvre.
* Ils participent à la sensibilisation de l’ensemble des acteurs à l’importance du contrôle interne.
* Ils proposent des plans de contrôle et suivent leur réalisation, exploitent les résultats.
* Ils analysent et suivent le traitement des incidents.
* **Les collaborateurs**
* Par leurs actions quotidiennes ils donnent vie au contrôle interne et assurent la maîtrise des risques.
* Ils respectent les procédures de travail formalisées.
* Ils mettent en œuvre les contrôles identifiés.
* Ils signalent les incidents et les anomalies dont ils ont connaissance.
  1. La filière fonctionnelle
* **Le pilote/ responsable du contrôle Interne**
* Il est le garant de la méthodologie et l’animateur de la démarche. Il en rend compte à la direction générale.
* Il élabore la méthodologie d’analyse de risques.
* Il met en œuvre un système de maîtrise des risques opérationnels conformément aux orientations de la direction.
* Il met en place, développe et anime le dispositif de contrôle interne.
* Il assure le maintien du système de management de la maîtrise des risques opérationnels et son évolution.
* Il conseille les correspondants contrôle interne et les forme à la méthodologie.
* Il anime une réunion *a minima* annuelle pour faire le bilan du contrôle interne avec les correspondants.
* **L’audit interne**
* Il porte un regard indépendant sur la construction du dispositif de contrôle interne et son efficacité.
* Il évalue le fonctionnement global du dispositif de contrôle interne et propose des axes d’amélioration.
* Il identifie éventuellement de nouveaux risques.
* Il vérifie la réalité des contrôles effectués et la fiabilité de la remontée des résultats des contrôles.

1. Le déploiement du contrôle interne et son manuel

Le dispositif de contrôle interne de l’office est matérialisé par différents documents qui permettent de décrire les activités de l’office, le rôle des acteurs et leurs droits et habilitations, de recenser nos principales procédures, de matérialiser les plans de contrôles.

Ces éléments qui viennent en complémentarité et en cohérence avec la cartographie des risques et sont structurés autour des documents suivants :

* un organigramme fonctionnel nominatif,
* un répertoire des habilitations SI,
* un logigramme,
* une procédure détaillée,
* un plan de contrôles,
* un répertoire du corpus documentaire.
  1. Organigramme fonctionnel nominatif

**L’organigramme fonctionnel nominatif permet :**

* d’identifier le rôle des acteurs prenant part au processus,
* de matérialiser les liens hiérarchiques entre les différents acteurs et les contrôles/vérifications hiérarchiques opérés,
* de matérialiser le respect du principe de séparations des tâches,
* de recenser les personnes ayant des autorisations de signatures d’engagement de dépenses dans le cadre du système de délégations prévues pour les OPH à l’article R421-18 du CCH.

Il est mis à jour lors de toutes modifications de l’organisation.

Figure : Exemple d’organigramme fonctionnel



* 1. Habilitations dans les systèmes d’information

Le recensement des habilitations dans le système d’information et notamment sur les applications métier consiste à établir une procédure de revue périodique des comptes génériques pour s’assurer que ces comptes sont limités et justifiés.

Une procédure de revue périodique (a minima 1 fois par an) des comptes nominatifs (administrateurs, utilisateurs) est documentée. Elle vise à s’assurer :

* du respect de la procédure de validation et approbation de la demande d’habilitation,
* du rattachement effectif à la structure des collaborateurs pour lesquels des comptes sont actifs,
* de l’exactitude des différentes informations liées au collaborateur (identification des droits dans le système d’information des personnels ayant accès au système d’information utilisé par le processus),
* de la pertinence des habilitations en fonction des missions exercées par les acteurs dans le cadre du système de délégations prévues pour les OPH à l’article R421-18 du CCH qu’ils ont reçues (composition des droits d’accès et leur implémentation dans les systèmes d’information répondent aux besoins opérationnels),
* du respect de la matrice des incompatibilités entre les rôles détenus par un même acteur. (Principe de séparations des tâches dans le système d’information).

seui

Figure : Exemple de matrice d’habilitation



* 1. Logigramme

**Le logigramme permet :**

* de matérialiser visuellement l’enchainement des tâches et les acteurs impliqués dans le processus,
* de recenser sous forme visuelle : les étapes et acteurs clés, le point d’entrée et de sortie d’un processus, les outils SI, les documents, et les contrôles de 1ier niveau associés à chaque étape du processus.

Figure : Exemple de logigramme





* 1. Procédure détaillée

L’objectif est de formaliser une fiche d’identité du processus résumant l’ensemble des informations clés le composant : pilote, objectif, données d’entrée et de sortie, outils, procédures liées, description littéraire du processus.

Figure  : Exemple de procédure détaillée

* 1. Plan de contrôles

**Le plan de contrôles permet :**

* de matérialiser l’ensemble des contrôles clés opérés, les acteurs, la nature et la fréquence de contrôle,
* de faire le lien entre les contrôles opérés et les risques identifiés dans la cartographie :
* identifier les éventuelles absences de contrôles par rapport à la cartographie des risques,
* identifier les éventuels risques couverts par des contrôles existants mais non référencés dans la cartographie.

Figure : Exemple de plan de contrôles



* 1. Documentation

**Le recensement de la documentation clé liée au processus permet :**

* d’inventorier le corpus documentaire clé associé au processus,
* d’identifier les documents à mettre à jour.

Figure : Exemple de matrice de recensement de la documentation



Table des figures

[Figure 1 : Pyramide du COSO (Committee Of Sponsoring Organisation of the tradeway commission) 6](#_Toc72778238)

[Figure 2 : Cadre de référence de la gestion des risques – FERMA (Federation of European Risk Management Associations) 8](#_Toc72778239)

[Figure 3 : les lignes de maîtrise 9](#_Toc72778240)

[Figure 4 : la pyramide du COSO 11](#_Toc72778241)

[Figure 5 : Articulation des différentes cartographies autour de l’univers des risques 15](#_Toc72778242)

[Figure 6 : Univers des risques 16](#_Toc72778243)

[Figure 7 : Diagramme temporel élaboration des cartographies 20](#_Toc72778244)

[Figure 8 : Matrice des risques bruts 23](#_Toc72778245)

[Figure 9 : Matrice de priorisation des risques 25](#_Toc72778246)

[Figure 10 : Exemple de plans d’actions 26](#_Toc72778247)

[Figure 11 : Exemple de plan de contrôle 26](#_Toc72778248)

[Figure12 : Exemple d’organigramme fonctionnel 29](#_Toc72778249)

[Figure13 : Exemple de matrice d’habilitation 30](#_Toc72778250)

[Figure14 : Exemple de logigramme 31](#_Toc72778251)

[Figure 15 : Exemple de procédure détaillée 32](#_Toc72778252)

[Figure16 : Exemple de plan de contrôles 32](#_Toc72778253)

[Figure17 : Exemple de matrice de recensement de la documentation 33](#_Toc72778254)

Table des tableaux

[Tableau 1 : Description des risques stratégiques 17](#_Toc72778230)

[Tableau 2 : Description des risques financiers 18](#_Toc72778231)

[Tableau 3 : Description des risques opérationnels 18](#_Toc72778232)

[Tableau 4 : Description des périls 19](#_Toc72778233)

[Tableau 5 : Exemple d’échelle pour la cotation de la probabilité 21](#_Toc72778234)

[Tableau 6 : Exemple d’échelle pour la cotation de l’impact 22](#_Toc72778235)

[Tableau 7 : Exemple de grille pouvant être utilisée pour évaluer les risques 23](#_Toc72778236)

[Tableau 8 : Exemple d’échelle pour les cotations des éléments de maîtrise 25](#_Toc72778237)

1. Source site internet de l’ANCOLS : <https://www.ancols.fr/page/controle-et-evaluation>

   L’article L 342-2 du code de la construction et de l’habitation précise au I, 1°, d) que l’agence a pour mission de contrôler individuellement et thématiquement le contrôle interne. [↑](#footnote-ref-1)
2. 40 000 euros HT à la parution du présent guide, décembre 2023 [↑](#footnote-ref-2)