COMMISSION DE
L'OCÉAN INDIEN

MANUEL DE CONTRÔLE INTERNE DE LA COMMISSION DE L'OCEAN INDIEN

Numéro du Document	COI/GRC/2024/001
Version	3.0
Date d'Entrée en Vigueur	06/11/2024
Préparé Par	Assistant technique Horizon 2030 / Direction / Comité d'accréditation
Approuvé Par	Secrétaire général

COMMISSION DE L'OCÉAN INDIEN

SOMMAIRE

LISTE DES ABRÉVIATIONS

- AECR : Auto-évaluation du contrôle des risques
- COPL : Comité des Officiers Permanents de Liaison
- COSO : Committee of Sponsoring Organizations of the Treadway
- COI : Commission de l'Océan Indien
- DGR : Département responsable de la gestion des risques
- GRC : Gouvernance, Risque, Conformité
- CGRO : Cadre pour la gestion des risques organisationnels
- SCI : Système de contrôle interne

I. PRÉAMBULE

Ce Manuel se réfère aux cadres juridique et institutionnel pertinents de la COI pour la mise en œuvre du système de contrôle interne au sein du Secrétariat général :

- Décisions des instances se rapportant à l'organigramme du Secrétariat général de la COI ;
- Règlement intérieur du Conseil des ministres de la COI ;
- Règlements financiers de la COI ;
- Règlement intérieur du Comité d'Audit et de Risques et mandat dudit Comité ;
- Charte d'Audit Interne de la COI ;
- Code de prévention et de lutte contre les pratiques prohibées ; et
- Cadre de Gestion de Risques Organisationnels de la COI.

1. Rappelant le rôle crucial de la Commission de l'océan Indien (COI) dans la promotion de la coopération régionale entre ses États membres, il est impératif que l'organisation adopte et maintienne des normes de gestion de risques et de contrôle interne au plus haut niveau. Le contrôle interne est une responsabilité partagée entre le Secrétariat Général, les Comités de la COI, les départements opérationnels, ainsi que l'ensemble du personnel.

2. Ce manuel de contrôle interne est fondé sur les principes universellement reconnus du cadre COSO (Committee of Sponsoring Organizations of the Treadway Commission), ainsi que sur les recommandations de l'Institute of Internal Auditors (IIA) concernant le modèle des trois lignes de défense. Ces référentiels sont essentiels pour garantir la gestion efficace des risques, la conformité aux normes internationales, et la responsabilisation à tous les niveaux de l'organisation.

3. En tant qu'organisation intergouvernementale, la COI opère dans un contexte géopolitique complexe qui exige des processus de contrôle interne rigoureux et flexibles, capables de répondre aux divers défis régionaux et internationaux. Le présent manuel offre un cadre structuré qui intègre les besoins spécifiques de l'organisation tout en permettant une gestion proactive des risques.

4. Le présent Manuel repose sur les meilleures pratiques et sur le cadre de contrôle interne universellement reconnu, élaboré et actualisé par référentiel COSO. Ce Manuel s'articule autour des cinq composantes suivantes :
   (a) L'environnement de contrôle : promouvoir une culture éthique forte et un engagement envers l'intégrité ;

(b) L'évaluation des risques : identifier, analyser et atténuer les risques qui pourraient affecter la réalisation des objectifs de la COI ;
(c) Les activités de contrôle : mettre en place des mécanismes qui assurent l'application des directives et des politiques institutionnelles. ;
(d) L'information et la communication : garantir que les informations pertinentes sont échangées en temps opportun pour soutenir la prise de décision ; et
(e) Les activités de surveillance : évaluer régulièrement l'efficacité des contrôles internes et apporter des ajustements si nécessaire.

5. La mise en œuvre de ce cadre de contrôle interne contribue à l'amélioration continue des systèmes et des processus de la COI, tout en veillant à ce que les objectifs de la Commission, notamment en matière de développement durable, de sécurité, de résilience économique et de coopération régionale, soient atteints de manière efficace et transparente.

6. Ainsi, le présent manuel s'inscrit dans une volonté de garantir une gouvernance exemplaire, tout en renforçant la confiance des partenaires techniques et financiers, des États membres, et des autres parties prenantes envers la COI.

II. INTRODUCTION

1. Le contrôle interne relève de l'ensemble du personnel de l'organisation, ainsi que du Conseil des ministres, du Comité des Officiers Permanents de Liaison (OPL), du Secrétaire général et, par délégation des membres du Comité de direction (Secrétaire Général, Directeur, Chargés de Mission et chefs des services) dûment identifiés, du comité d'audit et risques, du comité budgétaire, des auditeurs internes, du responsable de la gestion des risques et des départements opérationnels[1]. Collectivement, ils s'emploient à garantir de manière raisonnable la réalisation des objectifs fixés par la COI.

2. Le contrôle interne constitue un pilier fondamental pour garantir la réalisation des objectifs stratégiques de la COI, et ce, à travers l'application rigoureuse de procédures, de mécanismes de suivi et d'évaluation, ainsi que de systèmes de gestion des risques. Ce manuel s'appuie sur le référentiel COSO et les meilleures pratiques établies par l'Institute of Internal Auditors (IIA). Il définit des processus permettant de gérer les risques, de renforcer l'efficience et l'efficacité des opérations, de garantir la fiabilité des rapports financiers, et de veiller à la conformité aux engagements contractuels et législatifs.

3. Le manuel de contrôle interne de la Commission de l'océan Indien (COI) a pour objectif de fournir un cadre formel et cohérent pour garantir l'efficacité des contrôles internes au sein de l'institution. Ce manuel s'inscrit dans une démarche visant à renforcer la

[1] Domaine d'intervention

gouvernance, la gestion des risques, et la conformité aux normes internationales. Il permet à la COI d'assurer la transparence, la protection des actifs, et l'atteinte des objectifs fixés dans ses différentes missions et projets, tout en respectant les lois et règlements en vigueur.

4. L'application rigoureuse de ce manuel permettra à la COI de maintenir un environnement de contrôle solide et d'adopter une approche proactive pour la gestion des risques, en assurant l'engagement de l'ensemble du personnel et des parties prenantes dans le processus de contrôle interne.

5. La COI s'engage à mettre en place et à maintenir un système de contrôle interne (SCI). Ce SCI englobe le déploiement d'un dispositif de contrôle efficace à un coût raisonnable, permettant de fournir des informations cruciales sur les déficiences afin que le Secrétaire général, et par délégation, le (s) membre(s) du Comité de direction à qui la tâche sera confiée, puissent prendre rapidement des mesures correctives. Plus précisément, le système de contrôle interne et ses modalités de fonctionnement doivent fournir au Conseil de la COI, au COPL et au Comité de direction les moyens de :

   (a) Faire avancer la réalisation des buts et objectifs de la COI ;
   (b) Vérifier l'efficience et l'efficacité des opérations de la COI ;
   (c) Renforcer l'amélioration continue de l'efficience et de l'efficacité des systèmes et processus ;
   (d) Remplir leurs obligations en matière de responsabilité de contrôle ;
   (e) assurer la fiabilité et l'exhaustivité des informations portant sur les finances et la gestion de la COI ;
   (f) Respecter les politiques, lois et règlements en vigueur ;
   (g) Préserver les actifs ;
   (h) Réduire les risques opérationnels ; et
   (i) Rendre fidèlement compte des résultats financiers et opérationnels.

6. Le cadre de contrôle interne est étroitement lié au cadre de gestion des risques organisationnels (CGRO) de la COI.

7. Le présent Manuel est lié à tous les cadres et procédures adoptés par le Conseil de la COI et le Comité des OPL, ainsi que toutes les procédures internes du Secrétariat Général, mais plus particulièrement aux suivants :

   (a) Cadre de gestion des risques opérationnels ;
   (b) Cadre en matière de technologies de l'information ;
   (c) Code d'éthique ;
   (d) Code de prévention et de lutte contre les pratiques prohibées ;
   (e) Charte de lutte contre les discriminations, les harcèlements et les violences sexuelles ;

(f) Règles d'exclusion d'accès aux financements ;
(g) Charte d'audit interne.

8. Ces cadres et procédures sont publiés sur le site web de la COI.

III. CHAMP D'APPLICATION

1. Le présent Manuel s'applique à l'ensemble du personnel et des collaborateurs au sein de la COI. Il devra être respecté dans tous ses aspects, avec la pleine conscience que toute infraction a ses dispositions pourrait entrainer des pertes importantes pour la COI et exposer à des risques juridiques et financier indésirables.

IV. LE SYSTÈME DE CONTRÔLE INTERNE (SCI)

4.1 Environnement de contrôle

1. Il s'agit de la fondation du contrôle interne. À la COI, l'environnement de contrôle est basé sur un engagement fort envers des valeurs éthiques, l'intégrité et une culture de responsabilité. L'ensemble des intervenants doit incarner ces valeurs et promouvoir un climat de transparence et d'exemplarité à tous les niveaux de l'organisation. Le cadre d'éthique est mis en place pour guider le comportement des employés et garantir que les décisions sont prises dans le meilleur intérêt de l'organisation et de ses États membres.
2. L'environnement de contrôle constitue la base du système de contrôle interne au sein du Secrétariat général de la Commission de l'Océan Indien (COI). Il définit les valeurs, les principes éthiques, et les structures de gouvernance qui guident les actions de l'organisation dans la réalisation de ses objectifs. Un environnement de contrôle solide garantit que l'intégrité, la transparence et la responsabilité sont au cœur des activités de la COI, tout en assurant une gestion efficace des risques et une conformité aux standards internationaux.
3. Concernant la culture et valeurs éthiques, la COI s'engage fermement à promouvoir une culture organisationnelle fondée sur des pratiques éthiques, la transparence et l'intégrité. Ces valeurs constituent le socle de l'environnement de contrôle et sont essentielles pour instaurer la confiance auprès des États membres, des partenaires financiers et des parties prenantes.
4. Les principaux aspects de la culture éthique de la COI sont les suivants :

(a) Engagement envers l'intégrité : Tous les membres du personnel, ainsi que les parties prenantes externes, doivent adhérer aux principes d'intégrité dans leurs actions. Les pratiques non éthiques, telles que la fraude, la corruption ou le conflit d'intérêts, sont strictement interdites.

(b) Responsabilisation : Chaque acteur au sein de l'organisation est responsable de ses actions et doit rendre compte de ses décisions et de ses activités. La responsabilisation contribue à minimiser les erreurs et à prévenir les pratiques abusives.

(c) Code de conduite : Un code d'éthique est en place pour guider le comportement des employés et des partenaires, en précisant les standards attendus en matière d'éthique. Ce code est régulièrement mis à jour pour tenir compte des évolutions légales et organisationnelles.

5. Pour renforcer cette culture éthique, la COI met en œuvre des programmes de sensibilisation et de formation réguliers à destination de ses employés, afin d'assurer une compréhension claire des politiques éthiques, des attentes organisationnelles, et des obligations de chacun en matière de contrôle interne.
6. Concernant la gouvernance et structure organisationnelle, la gouvernance à la COI est structurée de manière à garantir la séparation de tâches et la supervision efficace des activités de l'organisation. Chaque entité au sein de la COI joue un rôle essentiel dans la mise en œuvre et le suivi du système de contrôle interne.
7. Aperçu des principales composantes de la structure de gouvernance et leurs responsabilités :
   (a) Le Conseil des ministres : Il est l'organe décisionnel suprême et approuve les orientations stratégiques et les politiques de la COI. Il exerce une supervision générale des activités de la COI.
   (b) Le Comité des OPL : son rôle principal est de réunir les avis des administrations concernées sur les propositions d'activités du Secrétariat Général et de faire part des propositions émanant des États membres. Il passe en revue l'avancement des activités du Secrétariat Général et approuve ou modifie les nouvelles propositions d'activités.
   (c) Le Secrétariat Général : Il assure la gestion opérationnelle quotidienne de la COI. Il est chargé de la mise en œuvre des politiques et des stratégies approuvées par le Conseil des États membres.
   (d) Le Secrétaire Général est le garant de la mise en place effective des systèmes de contrôle interne. En tant qu'ordonnateur principal de la COI, il est le décisionnaire final pour l'ordonnancement des dépenses et la mise en œuvre des politiques, avec le pouvoir d'approuver ou de rejeter les décisions financières et opérationnelles.
   (e) Le Comité d'Audit et des Risques : Ce comité joue un rôle crucial dans la supervision des systèmes de contrôle interne et de gestion des risques. Il évalue l'efficacité des processus de contrôle, examine les résultats des audits internes et externes, et veille à ce que les risques identifiés soient traités de manière adéquate. Le comité assure une indépendance vis-à-vis des opérations quotidiennes pour fournir une évaluation objective du système de contrôle interne.
   (f) Le Comité Budgétaire : organe subsidiaire du Comité des OPL, il est chargé d'examiner et formuler des recommandations aux instances de la COI en vue de l'approbation du budget de fonctionnement de l'organisation ainsi que le plan triennal.
   (g) Les départements opérationnels et fonctionnels : Chaque département de la COI est responsable de l'application des principes de contrôle interne dans ses activités. Cela inclut la mise en œuvre des contrôles de première et de deuxièmes lignes, la gestion des risques opérationnels et la communication des informations pertinentes au Secrétariat Général et aux autres instances de supervision.
   (h) Le responsable de gestion des risques et de conformité joue un rôle clé dans la deuxième ligne de défense en renforçant les cadres et les procédures de conformité de la COI. Il collabore étroitement avec les différents départements, services, et projets pour assurer l'opérationnalisation et la mise en œuvre effective d'un système

intégré d'évaluation des risques et de leur atténuation. Son intervention garantit que les mesures de conformité sont respectées à tous les niveaux, contribuant ainsi à une gestion des risques rigoureuse et alignée sur les normes internes et internationales.

(i) Le Département d'Audit Interne : L'audit interne est une composante essentielle de la structure de gouvernance de la COI. Ce département est responsable de l'évaluation périodique de l'efficacité des contrôles internes et de la conformité aux politiques de gestion des risques. Il fait rapport directement au Comité d'Audit et des Risques, garantissant ainsi une indépendance opérationnelle.

8. Cette structure de gouvernance favorise une approche intégrée du contrôle interne, en permettant une répartition claire des responsabilités et en assurant que les décisions stratégiques et opérationnelles sont prises dans un cadre de contrôle rigoureux et transparent.

4.2 Évaluation des risques

1. La gestion des risques est essentielle pour identifier et analyser les événements pouvant entraver la réalisation des objectifs de la COI. La COI effectue une évaluation continue des risques internes et externes, y compris ceux liés à la gestion des projets régionaux, aux relations avec les partenaires internationaux, et à l'évolution des environnements politiques et économiques. La cartographie des risques et des plans de mitigation sont utilisés pour évaluer les probabilités d'occurrence et les impacts potentiels des risques identifiés.

2. L'Identification et évaluation des risques est une composante essentielle du cadre de contrôle interne de la COI. Le processus d'identification des risques consiste à recenser de manière systématique les risques auxquels l'organisation pourrait être confrontée, qu'ils soient stratégiques, opérationnels, financiers ou liés à la conformité. Chaque département est chargé d'identifier les risques qui lui sont propres en tenant compte des activités spécifiques qu'il gère. Pour identifier les risques, la COI adopte une approche proactive, intégrant les retours des parties prenantes, les résultats des audits internes et externes, ainsi que les analyses effectuées par les responsables de la gestion des risques. Les risques sont ensuite classés en fonction de leur probabilité d'occurrence et de leur impact potentiel sur l'organisation.

3. L'appétence et tolérance au risque est définie par le Secrétariat général, présenté et discuté au Comité d'audit et des risques, et validée par le Conseil des ministres. Elle correspond au niveau de risque que l'organisation est prête à accepter dans la poursuite de ses objectifs. Le Secrétariat général adopte le cadre de tolérance au risque qui reflète son engagement envers la réalisation des objectifs tout en minimisant les expositions indésirables aux risques. L'appétence au risque, quant à elle, se réfère à l'approche proactive de la COI pour prendre certains types de risques calculés, particulièrement dans ses programmes de développement et de coopération régionale. Le Secrétariat général doit régulièrement évaluer si les niveaux de risques acceptés sont alignés avec

les objectifs stratégiques et les capacités de gestion des risques de l'organisation.

4. La cartographie des risques est un outil central dans le processus d'évaluation des risques de la COI. Ce processus permet d'identifier, d'évaluer, et de classer les risques selon leur probabilité de survenance et leur impact potentiel. La cartographie des risques est réalisée sur une base annuelle, mais elle peut être actualisée de façon continue en fonction des nouveaux risques identifiés ou de l'évolution de l'environnement opérationnel. Chaque risque est évalué à l'aide d'une matrice des risques qui croise la probabilité et l'impact afin de déterminer les priorités d'intervention. Les risques jugés critiques sont ensuite intégrés dans un registre des risques, et des plans d'action sont élaborés pour assurer leur gestion. La cartographie des risques aide également à orienter les décisions stratégiques et à allouer efficacement les ressources pour la gestion des risques.

5. La gestion et atténuation des risques implique qu'une fois les risques identifiés et cartographiés, des mesures sont prises pour atténuer les risques de manière adéquate. La gestion des risques au sein du Secrétariat général de la COI repose sur la mise en place d'activités de contrôle spécifiques pour chaque risque, en fonction de sa gravité et de sa probabilité. Les activités de contrôle incluent des actions telles que la séparation des tâches, la vérification des transactions et la surveillance continue des processus à risque élevé.

6. Pour chaque risque critique, des plans d'action correctifs sont élaborés afin de réduire son impact ou sa probabilité d'occurrence. Ces plans sont suivis et mis à jour en fonction de l'évolution des risques et des résultats obtenus. Le Secrétariat général veille également à la mise en place de processus de suivi et de rapport pour évaluer l'efficacité des mesures d'atténuation et ajuster les stratégies en conséquence.

7. Enfin, l'audit interne joue un rôle clé dans la gestion des risques, en fournissant une évaluation indépendante des contrôles mis en place et en identifiant d'éventuelles faiblesses dans les processus de gestion des risques.

4.3 Activités de contrôle

1. Les activités de contrôle sont les actions concrètes mises en œuvre pour atténuer les risques identifiés. À la COI, ces contrôles incluent des procédures d'autorisation, des vérifications régulières, des rapprochements de comptes, ainsi que des contrôles automatisés via des systèmes d'information pour les opérations complexes. Ces activités visent à s'assurer que les directives des instances et/ou du Secrétariat général sont exécutées et que les objectifs opérationnels sont atteints dans un cadre sécurisé et contrôlé.

2. Les activités de contrôle constituent les actions mises en place pour garantir que les

directives ci-dessus mentionnées sont respectées et que les objectifs de l'organisation sont atteints. Ces contrôles se déclinent en trois catégories principales (types d'activités de contrôle) :

(a) Contrôles préventifs : Ces contrôles visent à éviter que des erreurs ou des fraudes ne se produisent. Ils incluent des procédures d'approbation avant toute transaction ou décision, la mise en place de politiques claires, et la formation des employés sur les risques et les meilleures pratiques.

(b) Contrôles détectifs : Ils sont utilisés pour identifier des anomalies ou des irrégularités après qu'elles se sont produites. Les rapprochements de comptes, les vérifications périodiques et les analyses de performance sont des exemples de contrôles détectifs.

(c) Contrôles correctifs : Ces contrôles interviennent après la détection d'un problème pour apporter une solution immédiate. Ils incluent des actions correctives telles que la révision des processus, la correction des erreurs comptables, ou la mise à jour des procédures.

3. Les activités de contrôle sont effectuées à tous les niveaux de la structure organisationnelle du Secrétariat général, à diverses étapes des processus opérationnels et dans l'environnement technologique. Elles peuvent être de nature préventives ou détectives et englober une panoplie d'activités manuelles et automatisées, tels que les autorisations et les approbations, les vérifications, les rapprochements de compte et les évaluations de performance opérationnelle.

4. La séparation des tâches est une mesure fondamentale pour prévenir les erreurs et les fraudes. Au sein du Secrétariat général de la COI, cette pratique implique que les responsabilités soient partagées entre plusieurs personnes, de sorte qu'aucun employé ne puisse à lui seul initier, approuver, et enregistrer une transaction. Par exemple, la personne qui approuve une dépense ne doit pas être la même que celle qui effectue le paiement ou qui enregistre la transaction dans le système comptable. Cela réduit le risque de fraude interne et d'erreurs non détectées. La séparation des tâches est généralement intégrée dans la phase de sélection et de définition des activités de contrôle. Lorsque la séparation des tâches n'est pas possible, le Comité de direction définit et met en œuvre des activités de contrôle alternatives.

5. Le Secrétariat général utilise divers outils et procédures de contrôle pour mettre en œuvre et surveiller ses contrôles internes. Ces outils incluent :
   (a) Des listes de contrôle pour les processus fiduciaires, contractuels et opérationnels.
   (b) Des systèmes informatisés (logiciel, progiciel, etc.) pour automatiser les contrôles.
   (c) Des audits internes réguliers pour évaluer l'efficacité des contrôles en place.

6. Les procédures de contrôle sont appliquées à des fréquences variées : certains contrôles sont réalisés de manière continue (vérification des transactions en temps réel), tandis que d'autres sont effectués périodiquement (audits mensuels ou annuels).

7. Le Secrétariat général sélectionne et déploie un éventail global d'activités de contrôle qui contribueront à la prévention et à l'atténuation des risques afin de porter la réalisation des objectifs à des niveaux acceptables. Ces activités de contrôle sont déployées sous la forme d'un programme formel de suivi et de production de rapports. Ledit programme se décline en listes de contrôle de chaque département (voir le modèle en annexe C), conformément à la procédure décrite au CGRO.

8. Au terme de l'AECR, les activités de contrôle doivent être en adéquation avec la composante évaluation des risques du SCI. Le Secrétaire général, en Comité de direction, en fonction du niveau de risque identifié précédemment, définit et met en œuvre les actions nécessaires à la prévention, au partage, à la réduction ou à l'élimination d'un risque spécifique considéré comme élevé en raison de sa probabilité de survenance et de son impact.

9. Les actions ou activités sélectionnées pour la prévention ou l'atténuation des risques sont axées sur des processus financiers et opérationnels pertinents ou sur des transactions qui comportent toutes les composantes du SCI.

10. Le cadre de gestion des risques établit :

    (a) la périodicité à laquelle les activités de contrôle sont réalisées dans les délais impartis ;
    (b) la description des actions ou des activités de contrôle ;
    (c) les départements et les membres du personnel qui sont chargés de la réalisation des activités de contrôle ; et
    (d) la preuve de la réalisation du contrôle (un document, le partage de services informatiques ou d'une application, un logiciel ou GRC ou l'externalisation de services).

11. Si les activités de contrôle sélectionnées impliquent l'utilisation de la technologie, les droits d'accès des utilisateurs autorisés doivent être configurés suivant la décision du Secrétaire général en Comité de direction et selon la nature des fonctions concernées. Les activités de contrôle de sécurité appropriées limitent l'accès du système uniquement aux utilisateurs autorisés. L'usage de la technologie peut également favoriser l'automatisation de certaines activités de contrôle.

12. Lors de la réalisation des activités de contrôle, des erreurs, des écarts et d'autres irrégularités peuvent être constatés. Ces faits doivent être analysés et signalés. Par conséquent, des mesures correctives doivent être envisagées et mises en œuvre. Ces irrégularités sont ensuite répertoriées pour faire l'objet d'un suivi dans un délai déterminé.

13. Les membres du personnel doivent mener à bien les activités de contrôle pertinentes

au sein de leurs départements. Lorsque le Secrétariat général procède à une réévaluation ou à une révision périodique des cadres et procédures, les activités de contrôle interne doivent être révisées en conséquence.

À titre d'exemple, si on procède à une mise à niveau du module du logiciel Sage comptabilité, en y intégrant des activités automatisées de contrôle de transactions, les activités de contrôle qui étaient précédemment effectuées manuellement deviendront redondantes et ne seront plus nécessaires.

4.4 Information et communication

1. Un système de communication transparent est indispensable au bon fonctionnement du contrôle interne. Le Secrétariat général veille à ce que des informations pertinentes et fiables circulent efficacement à tous les niveaux de l'organisation, ainsi qu'avec les États membres, les partenaires et autres parties prenantes. Les outils de communication incluent des rapports financiers, des notes internes et des plateformes numériques. Le personnel est informé sur les rôles et responsabilités en matière de contrôle interne afin de faciliter la mise en œuvre des processus.

2. Un flux d'information efficace est essentiel pour soutenir le contrôle interne à la COI. Les informations pertinentes doivent circuler rapidement et de manière transparente entre les différents niveaux de l'organisation afin de permettre une prise de décision éclairée. Cela inclut la communication entre le Secrétaire général, la Direction, les départements, et les parties prenantes externes, ainsi que la remontée d'informations critiques liées à la gestion des risques ou aux contrôles financiers.

3. Les systèmes de communication du Secrétariat général comprennent des canaux formels tels que les rapports internes (établi dans le cadre de suivi-évaluation du Secrétariat général), les réunions de coordination (Comité de suivi, Comité de gestion, comité de pilotage, etc.) et les réunions des comités d'audit et des risques. Ils incluent également des canaux informels qui permettent aux employés de faire remonter rapidement des informations sur des anomalies ou des préoccupations. Par ailleurs, il utilise des systèmes numériques sécurisés pour faciliter le partage d'informations à travers ses différents services et pour garantir une traçabilité des échanges.

4. Pour assurer la confidentialité et l'intégrité des données et des informations sensibles, la Secrétariat général met en place des mécanismes de protection tels que le chiffrement des données, la gestion des droits d'accès, et l'utilisation de systèmes sécurisés pour stocker et transmettre les informations critiques. Ces mesures garantissent que seules les personnes autorisées peuvent accéder aux informations sensibles, et que les données financières et opérationnelles restent fiables et précises.

4.5 Activités de surveillance

1. La surveillance continue des activités de contrôle interne est réalisée via des audits internes et externes ainsi que par des mécanismes d'auto-évaluation. Le Secrétariat général met en place des examens périodiques pour s'assurer que les systèmes de contrôle restent efficaces face aux évolutions des risques et des besoins organisationnels. Les résultats de ces évaluations sont communiqués au Secrétaire général, qui s'assure de la mise en place d'actions correctives en cas de défaillances identifiées.

2. Le Secrétariat général met en place des mécanismes de surveillance continue pour s'assurer que les contrôles internes sont appliqués de manière appropriée et restent efficaces dans le temps. Cela comprend la réalisation d'audits internes périodiques ainsi que des évaluations ponctuelles lorsque des événements ou des changements importants surviennent (ex. introduction de nouveaux systèmes, modification des processus).

3. Les audits internes occupent une place centrale dans le dispositif de surveillance de la COI. Le Service d'audit interne procède à des évaluations régulières pour mesurer l'efficacité des systèmes de contrôle interne, détecter les éventuelles faiblesses, et proposer des recommandations concrètes visant à renforcer ces systèmes. Les auditeurs internes, bénéficiant d'une totale indépendance vis-à-vis de la direction, garantissent l'objectivité de leurs analyses. Ils rendent compte directement au Comité d'Audit et aux instances décisionnelles de la COI, assurant ainsi une transparence complète et une impartialité totale dans le suivi et l'amélioration des contrôles internes.

4. Lorsqu'une défaillance dans le système de contrôle est détectée, le Secrétariat général met en place un processus de suivi des défaillances pour s'assurer que des actions correctives sont prises rapidement. Les responsables concernés doivent élaborer un plan de remédiation détaillant les mesures à prendre, les délais d'exécution, et les ressources nécessaires. La mise en œuvre de ces actions est suivie jusqu'à leur achèvement pour éviter la récurrence des problèmes identifiés.

5. Les résultats issus des activités de surveillance peuvent être incorporés dans une section du rapport d'audit interne qui sera adressé au Comité d'Audit et de Risques.

6. Le Secrétaire général, le Comité d'Audit et de Risques et le Comité des OPL doivent être informés des défaillances détectées lors des activités de surveillance. Ces défaillances seront également communiquées aux responsables afin qu'ils prennent les mesures correctives nécessaires. Le Secrétaire général, ou le membre du Comité de direction auquel il aura délégué cette tâche, effectue un contrôle et un suivi pour s'assurer qu'il a bien été remédié aux défaillances à temps.

V. LIMITES DU CONTRÔLE INTERNE

1. Le système de contrôle interne, bien qu'efficace, présente des limites inhérentes. Celles-ci incluent le risque de collusion entre agents et collaborateurs, les erreurs humaines, et la possibilité que les différents responsables contournent les contrôles. Ces limites signifient qu'aucun système ne peut garantir une protection absolue contre les défaillances, la fraude ou les erreurs.

2. Il est essentiel de trouver un équilibre entre les coûts associés à la mise en place des contrôles internes et les bénéfices attendus. La COI doit veiller à ce que les contrôles ne deviennent pas excessivement lourds ou coûteux par rapport aux risques qu'ils visent à atténuer. La proportionnalité est cruciale pour garantir que les contrôles soutiennent efficacement les objectifs opérationnels sans freiner la productivité.

VI. RÔLES ET RESPONSABILITÉS

1. Le Secrétaire Général : il rend directement compte aux instances de la COI. Il s'assure de la mise en place, du déploiement et de la mise en œuvre d'un SCI performant. Il a l'autorité pour déléguer l'exécution des activités de contrôle à tous les niveaux du Secrétariat général de la COI.

2. Le Comité d'Audit et de Risques : il joue un rôle actif dans le contrôle de l'efficacité, de la disponibilité et du déploiement du SCI. Le COPL, par le biais du Comité d'Audit et de Risques, a le pouvoir d'interroger le Secrétariat général sur les rapports de contrôle interne, sur leur fonctionnement, sur des défaillances identifiées et doit veiller à ce que des mesures correctives soient prises en temps utile. Les principales fonctions du Comité sont décrites dans son règlement intérieur.

3. Le service d'audit interne : en tant que 3e ligne de défense, le service d'audit interne est appelé à garantir la fiabilité du système de contrôle interne et à fournir des conseils aux différents responsables au sein du Secrétariat général. Il évalue l'adéquation et l'efficacité des contrôles réalisés pour atténuer les risques identifiés conformément à la charte et au manuel d'audit interne.

4. Le responsable de la gestion des risques : il assiste et soutient les unités opérationnelles dans l'identification des risques connus et émergents. Il veille à ce que les risques présentant une forte probabilité de survenance et un impact élevé soient gérés de façon appropriée à tous les niveaux de l'institution par les principaux responsables concernés, qu'ils soient maintenus dans les limites des niveaux de tolérance établis, et s'assure de l'effectivité des contrôles adéquats. Nonobstant l'importance de ces responsabilités, cette deuxième ligne de défense n'a pas pour objectif l'exécution des contrôles mais elle vise à soutenir le SCI dans son ensemble.

5. Les départements opérationnels et fonctionnels : En tant que première ligne de défense, ils s'assurent de l'application du SCI dans leurs activités quotidiennes et ils jouent un rôle crucial dans la définition et l'actualisation des risques liés à leurs activités opérationnelles. Ils sont également tenus de participer à l'auto-évaluation du contrôle de risques.

6. Responsabilité du personnel : Tous les membres du personnel de la COI, quel que soit leur niveau hiérarchique, ont la responsabilité d'appliquer les cadres et procédures de contrôle interne. Ils doivent également signaler toute anomalie ou irrégularité via les canaux de communication appropriés. Le personnel opérationnel doit s'assurer que les contrôles sont intégrés dans leurs activités quotidiennes pour prévenir les erreurs et atténuer les risques.

VII. PROCEDURES D'AUTO-EVALUATION ET AMELIORATION CONTINUE

1. Le Secrétariat général de la COI a mis en place un processus structuré d'auto-évaluation permettant à chaque département d'évaluer régulièrement l'efficacité de ses systèmes de contrôle interne. Ce processus comprend l'utilisation d'outils tels que des questionnaires, des revues périodiques et des modèles d'audit standardisés, qui aident à identifier les lacunes, à proposer des améliorations et à ajuster les procédures de contrôle de manière proactive. Les résultats de ces auto-évaluations sont consolidés et analysés par le Service d'audit interne, qui joue un rôle clé dans la validation des améliorations proposées et dans le suivi de leur mise en œuvre, garantissant ainsi une amélioration continue du système de contrôle interne à l'échelle de l'organisation.

2. L'amélioration continue est un élément clé du système de contrôle interne de la COI. Des plans d'amélioration sont mis en place pour tenir compte des évolutions réglementaires, des meilleures pratiques internationales, et des leçons tirées des audits internes et externes. Ces ajustements permettent d'assurer que le contrôle interne reste pertinent et efficace à mesure que l'organisation évolue.

ANNEXES ET OUTILS PRATIQUES

1. Exemples de cadres et de procédures :
Le manuel de contrôle interne de la COI comprend des exemples de cadre sur l'éthique, la gestion des conflits d'intérêts, la lutte contre la fraude, et d'autres thèmes essentiels. Ces exemples servent de guides pratiques pour mettre en œuvre des contrôles efficaces.

2. Modèles d'évaluation des risques :
Des matrices d'évaluation des risques, des grilles d'auto-évaluation, et des listes de contrôle sont fournies pour aider à identifier et à classer les risques en fonction de leur probabilité et de leur impact. Ces outils sont destinés à faciliter le processus d'évaluation des risques à tous les niveaux de l'organisation.

3. Documents de référence :
Les procédures de contrôle interne de la COI sont également liées à d'autres documents de gouvernance, tels que les statuts, le règlement financier, et les règles internes. Ces références assurent que le contrôle interne est intégré dans les structures juridiques et organisationnelles de l'institution.

ANNEXE A. PROCÉDURE DE CRÉATION ET DE MAINTIEN DU SYSTÈME DE CONTRÔLE INTERNE

Chaque département procède à l'exécution, à la définition, à l'adaptation et à la mise à jour des activités de contrôle interne, suivant les étapes de l'AECR.

Tableau 1. Auto-évaluation en matière de contrôle de risques

Documentation & définition	Identification de risques	Évaluation et notation	Examen et approbation
1. Documenter l'environnement global de contrôle interne. 2. Définir l'entité faisant l'objet de l'AECR.	3. Identifier les risques importants. 4. Définir les principales activités de contrôle interne (CI) préventives ou d'atténuation de risques correspondantes.	5. Évaluer (tester) et noter les principales activités de CI. 6. Créer des plans d'actions correctives. 7. Attribuer une note de risque et de contrôle à chaque risque important sur une base résiduelle. 8. Attribuer une note de risque et de contrôle à l'entité faisant l'objet de l'AECR et présenter un rapport d'information sur l'AECR, le cas échéant.	9. Examiner les modèles de l'AECR après l'achèvement des évaluations et approuver les résultats de l'AECR. 10. Définir, sélectionner et mettre en œuvre les activités de contrôle interne préventives et d'atténuation de risques correspondantes, conformément au modèle établi.

Étape 1 - Documenter l'environnement de contrôle : la première étape de toute AECR consiste à documenter les risques et les contrôles visant à les atténuer. Une base de données centrale faisant office de registre principal de risques, est créée dans un document Word ou Excel, et actualisée pour répertorier tous les processus qui pourraient présenter un risque. Des fichiers comportant des activités de contrôle correspondantes de chaque département et visant à atténuer les risques, doivent également être constitués.

Étape 2 - Identification de risques : une fois l'environnement de contrôle défini au moyen du cadre et des outils appropriés (registres de risques, matrice de risques, listes des activités de contrôle interne), tous les processus opérationnels doivent être documentés, au cas où cela n'a pas encore été fait. L'étape suivante consiste à identifier les risques liés aux activités, aux processus et aux livrables de chaque département et responsable opérationnelle. Ces risques opérationnels sont généralement identifiés par les chefs de mission et les chefs de services assistés de leurs équipes. Ce processus est le résultat d'un effort collectif mené par le département chargé de la gestion des risques et tous les autres départements. Ils examinent les résultats des audits, les expériences précédentes et les observations externes pour cerner les éventuelles incidences négatives associées à chaque action. Cela permettra de normaliser la taxonomie des risques au sein de l'institution, et par ricochet, l'identification rapide, par l'équipe de direction, des risques importants l'affectant dans une grande mesure. Outre les risques opérationnels, les risques intégrés suivants doivent être maitrisés : le risque d'assurance, le risque de liquidité, le risque de marché, le risque de réputation, le risque stratégique et le risque de conformité.

Étape 3 - Évaluation des risques : une fois les risques identifiés, l'étape suivante consiste à les évaluer et à les noter. L'évaluation est une activité indispensable dans la mesure où le Secrétaire général, ou le responsable auquel il délègue cette tâche, sur avis du Département en charge de la gestion des risques (DGR), doit procéder à la hiérarchisation des risques, déterminer leurs mesures d'atténuation et présenter un rapport sur les risques majeurs. Au cas où un risque pourrait fortement être préjudiciable à l'organisation, il devra être maîtrisé avant les autres risques. Le chef de chaque département évaluera les risques auxquels son département est confronté, en fonction de leur probabilité de matérialisation et de leur impact.

Étape 4. Identification et évaluation des contrôles : les contrôles permettant d'atténuer les risques doivent également être identifiés et évalués. Cet exercice est beaucoup plus aisé que l'identification des risques car les contrôles ont été définis ou ont probablement déjà été instaurés par le Secrétaire général. Une évaluation doit être effectuée si des activités de contrôle n'ont pas été prévues pour un risque donné. Une liste de contrôle de chaque département doit être actualisée (voir l'annexe C) et le DGR pourra vérifier l'efficacité des contrôles sélectionnés. Les questions suivantes doivent être abordées : a) le contrôle permet-il d'atténuer le risque concerné ? b) Le contrôle est-il effectué assez fréquemment ? c) La personne qui effectue le contrôle dispose-t-elle des compétences et de l'expérience nécessaires et comprend-elle clairement la nature et l'objectif dudit contrôle ? d) Des problèmes ont-ils déjà été observés en raison de l'ineffectivité de ce contrôle ? L'évaluation de l'efficacité du contrôle peut porter

sur une population définie, un échantillon et sur une période donnée. Les contrôles peuvent alors être jugés efficaces ou non, ou nécessiter des ajustements, comme indiqué ci-dessous.

Étape 5. Mesures correctives : les AECR sont réalisées pour permettre à la COI de déceler et de combler les lacunes éventuelles dans les mécanismes de contrôle existants. L'identification de nouveaux éléments significatifs entraînant une aggravation des risques peut donner lieu à un examen plus approfondi et à la prise de mesures correctives, telles que la modification des activités de contrôle ou le déclenchement d'autres signaux d'alerte (pertes, fraude, etc.). Les mesures correctives sont adoptées à la suite d'événements spécifiques, d'une évaluation et d'une hiérarchisation des risques, et de contrôles effectués dans les différentes structures de l'institution. Cela permettra aux responsables de déterminer des plans d'action.

Notation	Description	Indicateurs de résultats
Contrôle effectif	Le dispositif de contrôle a été bien conçu et fonctionne en grande partie comme prévu.	• **Le contrôle permet d'atténuer sensiblement le risque comme prévu.**
Améliorations nécessaires	Une lacune a été relevée dans la conception et/ou le fonctionnement du dispositif de contrôle, qui de ce fait, n'atténue que partiellement le risque.	• **Le contrôle présente des lacunes.** • **Le contrôle ne permet pas de réaliser pleinement l'atténuation des risques attendue.** • **Il a été constaté que le contrôle n'est pas totalement efficace.**
Contrôle ineffectif	**Une lacune a été relevée dans la conception et/ou le fonctionnement du dispositif de contrôle et celui ne permet pas une atténuation adéquate des risques.**	• **Le contrôle ne permet pas d'atténuer les risques comme prévu.** • **Des preuves ont été apportées sur l'inefficacité du dispositif de contrôle (en termes de sa conception et/ou de son fonctionnement) ou l'ineffectivité du contrôle a été observée lors du suivi du contrôle ou à l'occasion d'événements internes récents et d'autres événements déterminants.**

Étape 6 - Suivi de l'AECR : il est important de suivre les résultats issus des rapports AECR de l'organisation. Le département chargé de la gestion des risques joue un rôle majeur dans ce domaine. Il examine les conclusions relatives aux risques, soutient le processus d'évaluation et de notation de risques grâce à la matrice. Il est chargé de la tenue des registres de risques, en vue d'une production de rapports. Il émet des avis sur les activités de contrôle interne définies et sélectionnées par les responsables et départements en fonction des risques qu'elles estiment critiques, à titre de mesures d'atténuation. Le Secrétaire général, en Comité de direction, approuve le SCI, l'évaluation des risques et les activités de contrôle interne sélectionnées. Le COPL, par le biais du Secrétariat général et du Comité d'Audit et de Risques, veille à la mise en place, à la disponibilité et au fonctionnement optimal du SCI. Un rapport annuel sur le contrôle interne devra être rédigé par le DGR afin d'assurer la réalisation effective des contrôles internes, ce qui permettra au COPL et au Secrétariat général de mener à bien leurs missions respectives.

ANNEXE B. MODÈLE D'AUTO-ÉVALUATION DU CONTRÔLE DES RISQUES

Catégorie de risques	Risques	Description	Fréquence (probabilité de survenance)	Impact	Mesures d'atténuation (activités de CI ou toute autre activité)
Risques financiers			Sur une échelle de 5	Sur une échelle de 5	
Risques opérationnels			Sur une échelle de 5	Sur une échelle de 5	
Risques de conformité			Sur une échelle de 5	Sur une échelle de 5	
Risques stratégiques			Sur une échelle de 5	Sur une échelle de 5	

ANNEXE C. MODÈLE DE LISTE DE VÉRIFICATION DES ACTIVITÉS DE CONTROLE INTERNE

Département XYZ							
Numéro d'identification du contrôle	Objet	Description	Fréquence	Chargé du contrôle	Politique/ procédure	Rapport/Formulaire	**Preuve**