COMMISSION DE
L'OCÉAN INDIEN

CADRE DE GESTION DES RISQUES ORGANISATIONNELS

Titre du Document	Cadre de gestion des risques organisationnels
Numéro du Document	COI/GRC/2024/002
Version	1.2
Date d'Entrée en Vigueur	01/03/2025
Date de Révision	28/02/2026
Préparé Par	Responsable GRC / Direction
Approuvé Par	Secrétaire général

COMMISSION DE L'OCÉAN INDIEN

Table des matières

Chapitre 1 : Introduction

La gestion des risques organisationnels au sein de la Commission de l'océan Indien (COI) constitue un pilier essentiel pour garantir la réalisation des objectifs stratégiques et opérationnels de l'organisation. En tant qu'organisation intergouvernementale, la COI est exposée à divers risques organisationnels potentiels dans ses champs d'intervention et domaines d'activité.

Ce **cadre de gestion des risques organisationnels** vise à fournir une approche structurée pour identifier, évaluer et gérer les risques qui pourraient entraver la performance et la pérennité des activités de la COI. Inspiré du modèle **Committee of Sponsoring Organizations of the Treadway Commission** (COSO) et aligné sur les pratiques internationales de gestion des risques établies par **l'International Professional Practices Framework** (IPPF) de l'**Institute of Internal Auditors** (IIA), ce cadre repose sur la méthodologie des trois lignes de défense.

La **première ligne**, constituée par les départements opérationnels, identifie et gère les risques au quotidien. La **deuxième ligne**, assurée par la fonction de gestion des risques et conformité, soutient et encadre ces processus. La **troisième ligne**, l'audit interne, assure un suivi indépendant et fournit des recommandations pour l'amélioration continue du cadre.

Ce document est conçu pour être simple et accessible, afin que l'ensemble du personnel et des collaborateurs du Secrétariat général de la COI puisse l'adopter et l'appliquer efficacement.

1.1 Qu'est-ce que la gestion des risques ?

La gestion des risques consiste à anticiper les événements susceptibles de perturber les objectifs de l'organisation et à mettre en place des actions pour réduire ces incertitudes à un niveau acceptable. Elle permet d'améliorer la capacité d'une organisation à gérer efficacement les risques qui pourraient affecter ses activités stratégiques, opérationnelles et quotidiennes.

Ce processus repose sur l'identification, l'évaluation et la hiérarchisation des risques. Il vise à répondre aux questions suivantes :

- **Qu'est-ce qui pourrait mal tourner ?**
- **Que ferons-nous pour éviter ou atténuer ces risques, et comment réagir si l'un d'eux se concrétise ?**

La gestion des risques n'est pas une action ponctuelle, mais un cycle continu qui s'intègre dans la stratégie de l'organisation et son exécution. Elle couvre tous les aspects des activités de l'organisation, passées ou en cours, pour tirer des enseignements des événements passés et préparer l'avenir. Un système efficace de gestion des risques signifie que l'organisation :

- **Comprend les risques auxquels elle est exposée.**
- **A évalué les stratégies pour éviter, atténuer ou gérer ces risques.**

Chaque collaborateur est impliqué dans la gestion des risques. Chacun doit identifier les risques dans son domaine de responsabilité et participer à leur gestion en mettant en place des actions préventives. Si un risque se concrétise, un plan d'action doit être prêt pour y répondre efficacement.

Le but de ce cadre est de fournir aux collaborateurs de la COI les compétences nécessaires pour mettre en œuvre une approche globale et systématique de la gestion des risques. Ce cadre est conforme au modèle COSO et vise à :

- Réaffirmer l'engagement de la COI à l'égard de la gestion des risques.
- Intégrer cette gestion dans la gouvernance de la COI, en assurant une communication claire entre les départements opérationnels et le Secrétaire Général.
- Rendre chaque collaborateur responsable de la gestion des risques dans son domaine de travail.
- Encourager une approche cohérente et transparente de la gestion des risques au sein de toute l'organisation.

Chapitre 2 : Rôles et responsabilités

La gestion des risques au sein de la COI repose sur une répartition claire des rôles et des responsabilités, impliquant l'ensemble de l'organisation. Voici un résumé des rôles clés.

Secrétaire général (SG)

Le Secrétaire général supervise le système de gestion des risques organisationnels (GRO) de la COI. Il est responsable de l'efficacité de ce système et veille à ce qu'il soit structuré de manière à aborder les risques clés de manière stratégique. Ses principales responsabilités, lesquelles peuvent être déléguées au Directeur incluent:

- Piloter et superviser la GRO.
- Clarifier l'appétence au risque.
- Valider la priorisation des risques identifiés et s'assurer de la mise en œuvre des mesures correctives.
- Contribuer à la cartographie de risques et à la surveillance des risques majeurs.

Comité de direction (CoDir)

Le Comité de direction (Secrétaire général, Directeur, Chargés de missions et Chefs de services) est chargé de l'intégration de la gestion des risques dans les processus organisationnels de la COI, tels que la planification stratégique et financière, ainsi que la gestion des performances. Ils collaborent avec le Responsable des risques et conformité pour veiller à promouvoir une culture de conscience des risques.

Responsable des risques et conformité

Le Responsable des risques et conformité (au sein de la direction) évalue l'efficacité du système de gestion des risques et veille à la communication efficace des risques principaux en matière de Gouvernance, Risques et Conformité (GRC). Il supervise et contribuera à dispenser la formation du personnel en matière de GRO, contribue à la production des cartographies de risques et collabore avec le Comité d'audit et des risques pour garantir que les risques sont correctement gérés.

Agents et collaborateurs

Tous les agents et collaborateurs au sein du Secrétariat général de la COI doivent adhérer au processus de gestion des risques, identifier les risques opérationnels

et communiquer toute information pertinente au Responsable des risques et conformité. Ensemble, ils intègrent des actions de contrôle dans leurs processus pour minimiser les risques potentiels et contribuer à la réalisation des objectifs de l'organisation.

2.1 Formation et sensibilisation

Pour assurer la mise en œuvre efficace des rôles et responsabilités définis dans le cadre de la gestion des risques organisationnels (GRO) de la COI, un programme de formation et de développement est essentiel. Ce programme vise à doter toutes les parties prenantes des compétences, connaissances et expertises nécessaires pour identifier, analyser et gérer les risques.

Conscience du Risque

Une culture de **conscience du risque** est essentielle au succès du système de GRO. Cette culture doit être encouragée à tous les niveaux de l'organisation, notamment par le Comité de direction. Tous les agents et collaborateurs, dans leur travail quotidien, doivent non seulement reconnaître les risques mais aussi prendre des mesures proactives pour les gérer. En instaurant cette mentalité, la COI s'assure que les risques sont constamment évalués et maîtrisés, contribuant ainsi à la sécurité et à la pérennité de l'organisation.

Programme de formation

Le programme de formation inclura deux volets principaux :

1. **Formation de sensibilisation générale** : Elle sera destinée à tous les collaborateurs, leur permettant de comprendre les bases de la gestion des risques et leur rôle dans ce processus. Chaque collaborateur doit être conscient des risques potentiels liés à ses activités et des moyens de les atténuer.
2. **Formation technique spécialisée** : Pour le Responsable de la gestion des risques, comme les membres du Comité de direction, des formations plus approfondies seront proposées. Ces sessions porteront sur l'identification des risques complexes, leur priorisation et la mise en place de plans d'action pour les gérer.

Les formations seront dispensées par des experts internes ou externes et seront évaluées régulièrement pour assurer leur pertinence et efficacité. Le programme sera ajusté en fonction des nouveaux risques émergents et des besoins spécifiques de la COI.

Chapitre 3 : Risques et contrôles

La gestion des risques et des contrôles est une fonction essentielle au bon fonctionnement de l'organisation. En comprenant les différentes catégories de risques, les types de contrôles disponibles et en effectuant une évaluation claire des risques inhérents et résiduels, l'organisation peut non seulement se protéger contre les menaces mais aussi exploiter les opportunités de manière proactive. Une approche bien structurée garantit que les risques sont identifiés, évalués et contrôlés de manière efficace, permettant ainsi à l'organisation d'atteindre ses objectifs stratégiques et opérationnels.

3.1 Qu'est-ce qu'un risque ?

Un risque est défini comme une menace qui peut affecter la capacité d'une organisation à atteindre ses objectifs ou à mettre en œuvre ses stratégies de manière efficace. Il peut découler d'événements, d'actions ou d'inactions, et peut avoir des impacts variés sur l'organisation.

- **Risques externes** : Ces risques sont liés à des facteurs environnementaux sur lesquels l'organisation a peu ou pas de contrôle, comme :
    - L'évolution économique ou des marchés
    - La concurrence accrue
    - Les changements réglementaires ou juridiques
- **Risques internes** : Ceux-ci résultent de décisions prises au sein de l'organisation, affectant la gestion des ressources internes, par exemple :
    - Vols
    - Paiements en double
    - Accès non autorisé aux systèmes informatiques

- **Risques au niveau des entités** : Ces risques concernent des aspects stratégiques et macro-économiques qui affectent l'ensemble de l'organisation.
- **Risques au niveau des processus ou activités** : Ils sont spécifiques à certaines tâches ou processus, souvent liés à des activités de contrôle tangibles au sein de l'organisation.

3.2 Catégories de risques

Les risques peuvent être classés en différentes catégories selon leur nature et leurs impacts :

- **Stratégiques** : Ces risques sont liés à la stratégie globale de l'organisation et à la réalisation de ses objectifs à long terme.
- **Conformité** : Ils concernent le respect des lois, règlements et normes applicables à l'organisation.
- **Opérationnels** : Ils affectent directement la capacité de l'organisation à exécuter ses processus quotidiens et à atteindre ses objectifs.
- **Financiers** : Ceux-ci incluent des risques liés à la gestion financière, comme la liquidité, l'information financière ou les fluctuations des marchés.

3.3 Contrôles (Types, Nature, Risques inhérents et résiduels)

Un contrôle est une mesure mise en place pour atténuer ou gérer un risque, augmentant ainsi la probabilité que l'organisation atteigne ses objectifs. Les contrôles sont essentiels pour réduire les risques identifiés et assurer que les opérations se déroulent conformément aux attentes.

Types de contrôles

Les contrôles peuvent être classés en deux grandes catégories :

- **Contrôles préventifs** : Ils sont conçus pour empêcher les erreurs ou irrégularités avant qu'elles ne surviennent. Ils sont souvent considérés comme les plus rentables, car ils évitent les coûts associés à la correction des erreurs. Exemples :
    - Autorisation préalable des paiements

- Limitation d'accès aux systèmes informatiques

- **Contrôles de détection** : Ces contrôles interviennent après coup, identifiant et corrigeant les erreurs ou les problèmes. Ils permettent à l'organisation de repérer les écarts et de prendre des mesures correctives. Exemples :
  - Rapprochement des comptes
  - Comparaison des budgets avec les données réelles
  - Rapports d'exception

Nature des contrôles

Les contrôles peuvent être manuels ou automatisés, ou parfois une combinaison des deux.

- **Contrôles manuels** : Réalisés par des personnes, ils nécessitent une intervention humaine pour fonctionner efficacement. Exemples :
  - Un collaborateur effectue un rapprochement bancaire manuellement.
  - Un cadre supérieur compare les performances réelles avec les prévisions budgétaires.
- **Contrôles de systèmes** : Intégrés dans des systèmes informatiques, ils sont automatisés et permettent une vérification et un suivi continus. Exemples :
  - Limitation d'accès via des autorisations informatiques
  - Journalisation automatique des modifications apportées aux données

Risques inhérents et résiduels

L'évaluation des risques repose sur deux concepts clés : les risques inhérents et résiduels.

- **Risque inhérent** : C'est le risque brut auquel une organisation est exposée avant la mise en place de tout contrôle ou mesure d'atténuation.
- **Risque résiduel** : Il s'agit du risque qui subsiste après la prise en compte des contrôles et des mesures d'atténuation. Ce risque net est celui qui est effectivement géré par l'organisation.

La distinction entre ces deux types de risques permet à l'organisation de mesurer l'efficacité des contrôles en place et de déterminer si des ajustements sont nécessaires pour atteindre un niveau de risque acceptable.

Chapitre 4 : Le Cadre

4.1 L'univers du risque

L'univers du risque représente les différentes menaces potentielles qui peuvent affecter l'organisation. Ces risques sont classés en quatre grandes catégories : **financières**, **opérationnelles**, **stratégiques** et **de conformité**. Les décisions sur la tolérance au risque doivent être prises en fonction de l'impact potentiel sur l'organisation, selon des critères bien définis.

COMPOSANTE PRINCIPALE	SOUS-COMPOSANTE	EXEMPLES DE DOMAINES À RISQUES
FINANCIÈRE	Processus budgétaire	Modèle budgétaire, hypothèses, comité budgétaire, viabilité financière, expansion, ajustements, frais administratifs
	Trésorerie	Mobilisation de fonds, gestion des liquidités, actifs, viabilité financière, fonds de développement, fonds d'urgence, paiements
	Suivi et évaluation des performances	Système de suivi, rapports d'impact, évaluation des performances individuelles, primes, rapports de progrès
	Gestion des dépenses	Fonction d'approvisionnement, audit, réduction des coûts, contrôles internes, conflits d'intérêt, délégation de pouvoirs
	Comptabilité et audit	Politiques comptables, audit interne et externe, rapports financiers, consolidation, normes internationales, comité d'audit
OPÉRATIONNELLE	Actifs physiques	Usure, protection, assurance, entretien, radiation
	Technologie de l'information	Sécurité réseau, cyberattaques, plan de reprise après sinistre, gestion de bases de données, cloud
	Personnel et ressources humaines	Recrutement, gestion des talents, culture, organigramme, paie, plan de relève, conditions de travail
	Approvisionnement	Conflits d'intérêt, appels d'offres, transparence, relations avec les tiers, gestion des fournisseurs

	Communication	Stratégie de communication, relations publiques, image de marque, communication de crise
CONFORMITÉ	Code de conduite et éthique	Fraude, blanchiment d'argent, conflits d'intérêts, comité de discipline, lancement d'alerte
	Juridique et réglementaire	Conformité aux lois, lois du travail, protection des données, gouvernance
	Exigences des bailleurs	Mobilisation de fonds, audits, systèmes de contrôle interne, poursuites juridiques
STRATÉGIQUE	Partenariats	Mobilisation de fonds, collaboration avec partenaires, bailleurs, expansion, alignement stratégique
	Gouvernance	Sommet, conseil des ministres, audit, meilleures pratiques internationales, responsabilité
	Planning et allocation de ressources	Mobilisation de fonds, plans stratégiques, budgétisation, suivi et évaluation, gestion des risques
	Initiatives principales	Vision, stratégie d'expansion, fonds communs, alliances, partenariats

4.2 Déclaration d'appétit pour le risque (DAR)

La DAR définit le niveau de risque que le Secrétariat général est prêt à accepter dans la conduite de ses activités, en tenant compte des obligations de conformité et des exigences des normes et meilleures pratiques internationales. La COI adopte une approche équilibrée du risque, favorisant l'innovation et l'adaptabilité tout en assurant une gestion rigoureuse des risques susceptibles de compromettre la durabilité, la réputation et la conformité de l'organisation.

L'appétit pour le risque est un cadre évolutif qui fait l'objet d'une évaluation périodique. Le Responsable des risques et conformité est chargé de réaliser des évaluations en fonction des besoins exprimés par le Secrétaire Général ou le Directeur, par délégation du Secrétaire général.

Toute révision substantielle de l'appétit pour le risque sera soumise à validation par la Direction et intégrée aux processus de gouvernance existants.

Cette approche garantit que la COI dispose d'un cadre clair pour la prise de décision tout en conservant la flexibilité nécessaire pour s'adapter aux évolutions de son environnement.

Les principales catégories de risques et leur tolérance sont définies comme suit :

- **Risques stratégiques** (projets, partenariats, financements) : Tolérance modérée. La COI accepte un certain degré de risque stratégique pour innover et améliorer l'efficacité de ses actions, tout en restant alignée avec ses obligations et engagements institutionnels. *Toute déviation majeure de ses objectifs nécessite une validation au plus haut niveau (Instances décisionnelles).*
- **Risques opérationnels** (activités du Secrétariat et des DI) : Tolérance faible. La COI met en place des contrôles rigoureux pour réduire les risques opérationnels susceptibles d'affecter la continuité des activités et la qualité des services.
- **Risques de conformité** (normes juridiques, réglementaires et éthiques) : Tolérance très faible. La COI maintient une vigilance accrue afin d'assurer le respect des réglementations et engagements contractuels, et d'éviter tout risque pouvant compromettre sa crédibilité institutionnelle. *Toute infraction à la réglementation ou aux principes d'éthique entraîne des actions correctives immédiates et des sanctions si nécessaire.*
- **Risques financiers** (gestion budgétaire, financements externes) : Tolérance faible à modérée. La COI adopte une approche prudente pour la gestion des fonds, cherchant à minimiser les expositions financières non maîtrisées tout en garantissant l'optimisation des ressources disponibles. *Toute exposition financière doit être couverte par des mécanismes de contrôle et d'audit stricts.*
- **Risques informatiques et cyber** (sécurité des systèmes, protection des données) : Tolérance faible. Tout incident cyber doit être rapidement détecté et traité pour éviter toute fuite de données sensibles.
- **Risques de réputation** (image institutionnelle, communication publique) : Tolérance très faible. Toute atteinte à l'image de la COI doit être immédiatement corrigée avec une communication proactive et transparente.

4.3 Évaluation des risques et rapportage

L'évaluation des risques intervient après l'identification des événements et avant la réponse au risque. Son objectif est de mesurer la taille des différents risques, qu'ils soient individuels ou collectifs, afin de concentrer l'attention de la direction sur les menaces et opportunités les plus critiques. Cela permet de gérer les niveaux de risque dans les seuils de tolérance définis, sans contrôle excessif ni négligence d'opportunités importantes.

Étape	Description
1. Effectuer l'Évaluation des Risques	Processus collaboratif et systématique basé sur l'identification, l'analyse, et l'évaluation des risques, utilisant les meilleures informations disponibles, complétées par des enquêtes supplémentaires si nécessaire.
2. Identifier les Risques	Identification et reconnaissance des risques pouvant affecter les objectifs organisationnels. Des informations pertinentes et actuelles sont essentielles à cette étape.
3. Évaluer l'Importance et la Probabilité	Analyse et qualification des risques identifiés selon leur probabilité d'occurrence et la gravité de leurs conséquences.
4. Créer un Registre des Risques et Plan de Réponse	Un registre documente les risques, les contrôles, et les plans d'action. Il permet un suivi continu et la mise en œuvre des stratégies de gestion des risques.
5. Suivi et Évaluation	Le suivi permanent et l'évaluation régulière du processus de gestion des risques garantissent l'efficacité de la conception et de la mise en œuvre. Ils sont intégrés à chaque étape du processus, avec des responsabilités clairement définies. Le feedback continu permet des améliorations.

Tous les collaborateurs sont responsables de la gestion des risques dans leurs domaines respectifs, mais certaines fonctions sont attribuées à des personnes spécifiques. Le cadre global, les politiques et la conception de la gestion des risques organisationnels sont dirigés par le Responsable des risques et conformité. Un mécanisme de rapportage est en place pour identifier toute lacune dans les réponses aux risques et garantir que les actions correctives sont prises rapidement. Ces activités sont surveillées et rapportées à la hiérarchie du Secrétariat général de la COI, avec un rapport annuel destiné au Comité d'Audit et des Risques.

Le Comité d'Audit et des Risques a pour responsabilité de questionner la direction sur l'exhaustivité des risques identifiés, d'assurer que tout risque émergent est pris en compte et de surveiller la mise en œuvre des mesures de réduction des risques dans les délais prévus. Le comité veille également à ce que le système de gestion des risques de la COI soit aligné avec la stratégie de gouvernance. Le Secrétaire général a pour responsabilité de s'assurer que des mesures d'atténuation des risques sont formulées, avec des responsabilités clairement définies et des délais respectés.

Un rapport de risque annuel sera préparé par le Responsable des risques et conformité et le Comité d'audit et des risques, incluant une carte de chaleur des risques, des remarques importantes pour la direction, des rapports d'exceptions en annexe si nécessaire, ainsi qu'un registre des risques et des contrôles mis à jour.

Chapitre 5 : Analyse des risques

Un certain nombre de techniques ont été mises en œuvre par le Secrétariat général de la COI, avec l'aide d'un expert en Gouvernance, Risques et Conformité (GRC), pour identifier les risques au sein de l'organisation dans le cadre du projet INCA 1 (Renforcement des Capacités Institutionnelles) de fin 2018 à 2022.

5.1 L'identification des risques

Cette méthodologie sera reprise par le Responsable des risques et conformité pour les futures actualisations. L'expert GRC a procédé à une analyse approfondie des documents clés, incluant la stratégie, le cadre juridique, les politiques et procédures de la COI, ainsi que les rapports d'audit et les procès-verbaux des réunions de la direction. Cette analyse a permis de dresser une liste initiale des risques potentiels.

Un questionnaire a ensuite été envoyé aux parties prenantes clés, notamment le Secrétaire général, les Chefs de service, les Chefs de projet, les membres du Comité d'audit et des risques, ainsi que des parties prenantes externes. Les réponses ont été suivies d'entretiens approfondis, garantissant une couverture complète des domaines de risque potentiels. Cette démarche a abouti à la préparation d'une liste de risques, présentée lors d'un atelier sur les risques.

Cet atelier, organisé avec les participants concernés, a permis de revoir et hiérarchiser les risques identifiés. Les participants ont voté de manière anonyme pour prioriser ces risques. Ce processus a établi une base solide pour les futures évaluations et ajustements des risques.

5.2 Priorisation des risques

Après avoir identifié les risques, ceux-ci sont évalués en fonction de leur probabilité et de leur impact. Les risques sont évalués selon deux critères :

1. **La probabilité** ou la fréquence d'occurrence.
2. **L'impact** ou la gravité des conséquences pour la COI si le risque se réalise.

Noter les risques selon leur probabilité

Indice	Description	Fréquence	Probabilité
5	Très probable	Au moins une fois en 3 mois	L'événement devrait définitivement se produire.
4	Probable	Au moins une fois en 6 mois	L'événement va probablement se produire.
3	Possible	Au moins une fois en 1 à 5 ans	L'événement pourrait se produire.
2	Peu probable	Au moins une fois en 5 à 10 ans	Faible probabilité d'occurrence.
1	Très improbable	Au moins une fois en plus de 10 ans	Circonstances exceptionnelles.

Noter les risques selon leur impact

Indice	Description	Définition
5	Extrême	Perte financière > 30%, impact majeur et durable.
4	Élevé	Perte financière entre 15% et 30%, impact important.
3	Important	Perte financière entre 5% et 15%, impact modéré.
2	Modéré	Perte financière entre 1% et 5%, impact limité.
1	Faible	Perte financière < 1%, impact minime.

Les risques sont également classés en deux catégories :

- **Risque inhérent** : Risque existant avant toute mesure de contrôle.
- **Risque résiduel** : Risque restant après la mise en œuvre de ces mesures.

Classement des risques

Le score de **risque inhérent** est obtenu en combinant la note de probabilité et d'impact

Risque inhérent = Probabilité x Impact

Une fois les risques inhérents identifiés, il est essentiel d'évaluer les mesures de contrôle en place pour minimiser ces risques. Ces contrôles comprennent les politiques et procédures mises en œuvre pour réagir efficacement. L'efficacité de ces mesures est évaluée pour obtenir le **risque résiduel**, calculé de la manière suivante :

Risque résiduel = Risque inhérent / Efficacité du contrôle

Ainsi, les risques résiduels permettent de déterminer l'exposition restante de la COI après la mise en œuvre des contrôles, garantissant une évaluation continue et une gestion proactive. Lors de l'atelier, les participants votent sur ces éléments, et le score final est calculé, permettant de hiérarchiser les risques.

Une fois notés, les risques sont répertoriés sur une **carte de chaleur des risques**, qui permet de visualiser leur priorité de manière structurée. Cette carte facilite la prise de décision à tous les niveaux de direction de la COI, aidant à adopter une culture de prise de conscience du risque et à assurer une évaluation régulière des risques importants.

5.3 Réagir aux risques

Lorsque les contrôles existants ne réduisent pas suffisamment le risque pour rester dans les limites acceptables de la COI, ou lorsque de nouveaux risques émergent, ces risques sont remontés à la direction pour prise de décision. Les options de gestion des risques, appelées les « 4 T », sont :

1. **Accepter (Take)** : L'organisation accepte le risque s'il est inévitable ou s'il apporte une opportunité.
2. **Transférer (Transfer)** : Le risque est transféré via assurance, partenariats, sous-traitance ou couverture.
3. **Éliminer (Terminate)** : Arrêter l'activité ou ajuster les objectifs pour éliminer le risque.

4. **Traiter (Treat)** : Atténuer le risque à un niveau tolérable par des mesures organisationnelles, opérationnelles ou de surveillance.

Les décisions sur la gestion des risques tiennent compte de l'environnement, des objectifs de l'organisation, de la nature du risque, de l'appétit pour le risque, et du coût des actions possibles.

5.4 Registre des risques et Plans d'action

Après avoir déterminé les méthodes de traitement des risques, le Responsable des risques et conformité élabore un Registre des risques qui inclut au minimum :

- Les 25 à 30 risques identifiés par la direction
- Les notes d'impact, de probabilité et d'inhérence pour chaque risque
- Les contrôles d'atténuation en place pour les risques identifiés
- Les notes d'efficacité de ces contrôles
- Les notes de risque résiduel pour chaque risque
- Les mesures correctives à mettre en œuvre pour les risques insuffisamment atténués
- Les agents responsables de la mise en œuvre de ces mesures
- Les échéanciers associés à ces mesures et les principaux indicateurs de performance pour évaluer l'atténuation des risques
- Le niveau de tolérance actuel pour chaque risque (inacceptable, doit être amélioré, ou acceptable)

Le Registre des risques, les mesures à prendre, et l'état de leur mise en œuvre sont présentés au Comité d'audit et des risques pour suivi. Le Comité peut contester la Carte de chaleur ou le Registre des risques si nécessaire. Les versions finales de ces documents doivent être validées par le Comité d'audit et des risques.

Chapitre 6 : Cycle de gestion des risques

Le cycle de gestion des risques est un processus dynamique et systématique permettant à l'organisation d'identifier, d'évaluer, de traiter et de surveiller continuellement les risques. S'étendant sur trois ans, il intègre des évaluations régulières basées sur la gravité des risques identifiés. Un cycle bien structuré est

essentiel pour maintenir la résilience et l'efficacité de la COI, tout en favorisant une culture proactive de gestion des risques au sein de l'organisation.

Risques Élevés (1 an)

Les risques jugés élevés sont soumis à une évaluation annuelle. Cette fréquence d'évaluation garantit une gestion proactive, permettant à l'organisation d'adapter rapidement ses mesures de contrôle en réponse aux changements dans le contexte opérationnel ou réglementaire. Les actions correctives peuvent être mises en place rapidement pour atténuer les impacts potentiels, assurant ainsi la résilience des opérations.

Risques Moyens et Faibles (2-3 ans)

Les risques moyens et faibles sont examinés tous les deux à trois ans, en fonction de la stabilité du risque. Cette évaluation moins fréquente est justifiée, car ces risques ont un impact et une probabilité relativement faibles. Cependant, une surveillance continue est essentielle pour éviter qu'ils ne se transforment en problèmes majeurs.

Cycle Léger et Événements Déclencheurs

Un cycle léger est également intégré au processus de gestion des risques. Ce cycle est déclenché par des événements spécifiques, tels qu'une demande de modification de risque ou de contrôle émanant du Chef de service. Cette flexibilité permet de réagir rapidement à des changements significatifs dans le paysage des risques, garantissant que l'organisation reste adaptable et capable de gérer des situations imprévues de manière efficace.

Chapitre 7 : Modèles et Outils

7.1 Questionnaire d'évaluation des risques

Questionnaire d'identification de risques

N'hésitez pas à utiliser des pages supplémentaires si nécessaire afin de fournir le plus d'informations possibles à chaque question.

1. **Selon vous, quels sont les facteurs qui empêchent actuellement la COI d'atteindre ses objectifs ?**

2. **Selon vous, quels contrôles sont déjà en place pour atténuer ces risques ? Et quels contrôles devraient être introduits pour ce faire ?**

3. **Selon vous, quelles sont les principales opportunités dont dispose la COI pour se développer et réussir à l'avenir ?**

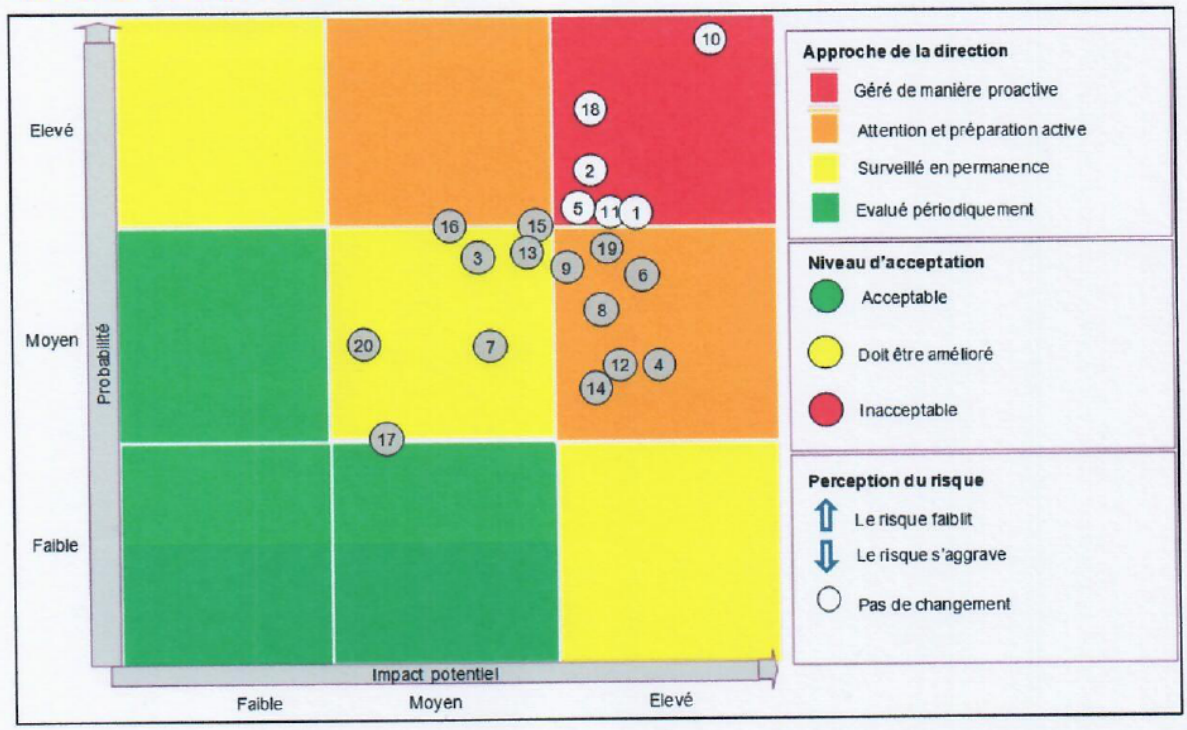
4. **Selon vous, quels facteurs nouveaux ou émergents pourraient empêcher la COI d'atteindre ses objectifs à l'avenir ?**

7.2 Registre des risques

Registre des risques
Commission de l'océan indien
Préparé par :
Date :

Unité	Catégorie de risque	Risque	Propriétaire du risque	Détails	Causes	Conséquences	Impact	Probabilité	Notation	Note de risque inhérent	Réf. De contrôle	Détail du contrôle	Indicateur-clef du contrôle	Type du contrôle	Note du contrôle	Propriétaire du contrôle	Fréquence opérationnelle	Conception du contrôle	Opération du contrôle	Risque résiduel – impact	Risque résiduel – probabilité	Risque résiduel – note	Conclusion	Changements du risque depuis le dernier trimestre	Plan d'action (« 4 T »)	Date de mise en œuvre	Agent responsable pour la mise en œuvre

7.3 Carte de chaleur des risques



7.4 Formulaire de modification des risques et contrôles

Formulaire de demande de modification de risque/de contrôle

Formulaire de demande de modification de risque/de contrôle			
Nouveau risque	**Oui/Non**	**Risque existant**	**Oui/Non**
Nom du Chef de service	< Indiquez le nom >	Date:	< Indiquez la date >
S'il s'agit d'un nouveau risque			
Description du risque	< Donnez la définition du risque >		
Contrôles existants	< Indiquez les contrôles existants capable d'atténuer le risque >		
S'il s'agit d'un risque existant			
Référence du risque	< Indiquez la référence du risque à partir du Registre des risques >		
Définition du risque	< Donnez une définition du risque à partir du Registre des risques >		
Zones de changement potentielles			
Domaine de gestion du risque	< Du domaine XY au domaine YZ et une explication des raisons de ce changement >		
Evolution du risque perçue	< De s'améliore/reste stable/s'aggrave à s'améliore/reste stable/s'aggrave et une explication des raisons de cette évolution >		
Contrôles d'atténuation	< Description des nouveaux contrôles > < Éliminer les contrôles redondants >		
État de mise en œuvre de l'action et remarques	• Mise en œuvre ; • En cours de mise en œuvre ; • Pas encore lancée ; ou • N'est plus valable.		
Autre	Changement de propriétaire de l'action, indicateurs-clefs de performance, délais, etc...		

Historique des Révisions

Version	Date	Description du Changement	Auteur
1.0	03/2021	Version initiale	INCA 1
1.1	11/2024	Appropriation et institutionnalisation du document	Responsable GRC
1.2	03/2025	Renforcement de la DAR après un trimestre	Responsable GRC

Contrôle du Document

Responsable du document	Responsable GRC / Direction
Date de Prochaine Révision	28/02/2026