Gestion du risque institutionnel (GRI) du PNUD
Politique et procédures

Date d'entrée en vigueur – 13/03/2019

Propriétaire de la politique : BMS/BPPS

Version approuvée, novembre 2018

Quoi de neuf

Les révisions apportées à la politique de GRI visent à améliorer les éléments suivants :

- ✓ Importance de cultiver une ***culture du risque*** au sein de l'organisation pour faciliter la prise de risques responsable et la prise de décisions éclairée
- ✓ ***Unité dans l'approche et la méthodologie*** utilisées pour la gestion des risques dans l'ensemble de la programmation et des opérations (y compris par un registre des risques commun)
- ✓ Favoriser la ***gestion des occasions***, la prévoyance et l'innovation plutôt que d'adopter une approche qui vise uniquement à prévenir les dommages et à réagir aux problèmes lorsqu'ils se présentent.
- ✓ Une ***meilleure harmonisation entre les catégories de risque et les critères de qualité de la programmation***, garantissant une gestion du risque et une assurance de qualité allant de pair.
- ✓ ***Maintenir une évaluation des risques simplifiée*** au niveau du projet, tout en assurant l'harmonisation avec la méthodologie de la GRI.
- ✓ Importance d'***harmoniser l'établissement de rapports sur les risques avec les cycles d'établissement de rapports existants*** au sein de l'organisation
- ✓ Introduction des « ***Trois lignes de défense*** » pour la gestion des risques et la gouvernance

Les modifications spécifiques incluent les éléments suivants :

Politique de la GRI 2016	Modification
Responsable de la politique : BMS	***Modifié*** pour propriété partagée de BMS et de BPPS en vue d'assurer une approche associant programmation et opérations.
Lenteur du processus **structurel et linguistique** de la politique	***Modification :*** Langage remanié pour alléger le processus et plus axé sur la définition des normes de GRI de qualité.
Termes et définitions	Définitions relatives au risque programmatique ***clarifiées*** et définitions séparées du texte de la politique.
Registre des risques dans le IWP et journal des risques du projet séparé dans Atlas	***Modification :*** Harmonisation entre le journal des risques du projet Atlas et le registre des risques du IWP. Proposition d'un système d'information sur les risques totalement intégré.
Modèle de critères de la GRI requis pour tous les niveaux de risque	Un modèle de critères de la GRI ***simplifié*** est introduit pour les projets, à intégrer dans le registre des risques.

Manque de clarté sur le processus d'**évaluation des risques** (identification, analyse, évaluation) au niveau du projet	***Clarification*** des éléments clés de l'évaluation des risques liés à la qualité, en veillant à l'établissement de liens avec les processus normatifs existants tels que la théorie du changement, le SES, le HACT, les évaluations de sécurité, etc. ***Clarification*** des exigences en mettant en place un processus de consultation et en impliquant les principales parties prenantes internes (p. ex., la programmation et les opérations) et externes. ***Clarification*** de la matrice de risques afin d'assurer une catégorisation harmonisée des risques à tous les niveaux.
Catégorisation des risques en GRI	***Modification :*** 8 catégories de risque, introduisant la sûreté et la sécurité en tant que nouvelle catégorie. Les catégories de GRI doivent être schématisées conformément aux critères de qualité de la programmation de façon à lier étroitement la gestion des risques et la qualité de la programmation.
Une définition large du risque, mais une interprétation étroite de la politique met	***Ajout :*** prise en compte des effets positifs de la gestion des risques et des occasions par le traitement des risques et le modèle de critères.
l'accent sur les ***effets négatifs*** du risque	
Les exigences en matière d'**établissement de rapports sur les risques** ne sont pas claires au niveau du projet	***Clarification :*** l'établissement de rapports sur les risques du projet est harmonisé avec les cycles d'établissement de rapports du projet (au minimum une fois par an).
Les structures de **gouvernance** de la GRI ne sont pas clairement définies	***Ajout :*** les trois lignes de défense pour une gestion efficace des risques, conformément au modèle de gestion des risques, de surveillance et de responsabilisation des Nations Unies
Procédures de GRI	***Ajout*** : un tableau des procédures de GRI, conforme au modèle POPP, afin de clarifier le processus et les rôles/responsabilités.

Table des matières

1. Champ d'application et objectifs de la politique

Naviguer dans la complexité de multiples incertitudes est au cœur de la quête du PNUD pour trouver des solutions novatrices aux problèmes de développement et d'organisation. Le système de gestion du risque institutionnel (GRI) du PNUD est conçu pour permettre à l'organisation d'être prospective et de gérer les effets des incertitudes sur les objectifs. Le but ultime de la GRI est de **garantir des décisions prospectives et tenant compte des risques** à tous les niveaux de l'organisation, maximisant ainsi les gains tout en évitant les pertes inutiles.

Le champ d'application de la politique de GRI couvre les risques à tous les niveaux de l'organisation, en tenant compte du contexte interne et externe. Le **risque** est défini comme étant l'effet de l'incertitude sur les objectifs organisationnels, pouvant être positif et/ou négatif (ISO 31000 :2018 ; voir l'annexe 1 pour tous les termes et définitions). Cela inclut les effets des activités du PNUD sur des facteurs externes, tels que les dommages causés aux personnes et à l'environnement. La GRI du PNUD accorde la priorité à la prévention et à la gestion des effets négatifs potentiels, mais cherche à maximiser les effets positifs dans la mesure du possible. La GRI du PNUD concerne ce qui suit :

- ***Risque institutionnel.*** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver l'efficience et l'efficacité des principales opérations au sein de l'organisation.
- ***Risque programmatique*****.** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver la réalisation des objectifs du programme ou du projet.
- ***Risque contextuel*****.** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver la progression vers les priorités en matière de développement d'une société donnée. La GRI prend en compte le risque contextuel lorsque ces incertitudes externes présentent également des risques institutionnels ou programmatiques.

La GRI applique une approche intégrée de la gestion des risques, avec une intégration horizontale pour tous les types de risques et une intégration verticale en provenance de projets jusqu'au niveau de l'entreprise. En introduisant une approche intégrée et systématique de la gestion des risques, la politique de GRI du PNUD vise à :

- Accroître l'**efficacité et la pertinence du programme** grâce à une prise de décision adaptative et éclairée
- Assurer une plus grande **assurance** quant à la gestion des risques importants
- Permettre l'exploration de **solutions innovantes** aux défis organisationnels et en matière de développement

- Influencer l'allocation efficace et ciblée des **ressources** là où le besoin se fait le plus sentir
- Renforcer la **réputation** du PNUD en tant qu'organisation axée sur les valeurs et tenant compte des risques
- Augmenter l'**efficacité** en préservant l'utilisation responsable des ressources
- Protéger **les personnes et l'environnement**
- Gérer et réduire à un niveau acceptable les risques pour la **sûreté et la sécurité** du personnel, des locaux et des biens du PNUD.

La politique de GRI du PNUD exige une approche intégrée de la gestion des risques dans l'ensemble de l'organisation, mais la gestion des risques est un processus partagé avec les partenaires. En particulier, les risques doivent être envisagés dans une perspective commune à l'ensemble du système des Nations Unies et examinés à chaque étape du processus du PNUAD et par une programmation conjointe (voir les directives du PNUAD). Les risques de sécurité sont gérés par le système de gestion de la sécurité des Nations Unies.

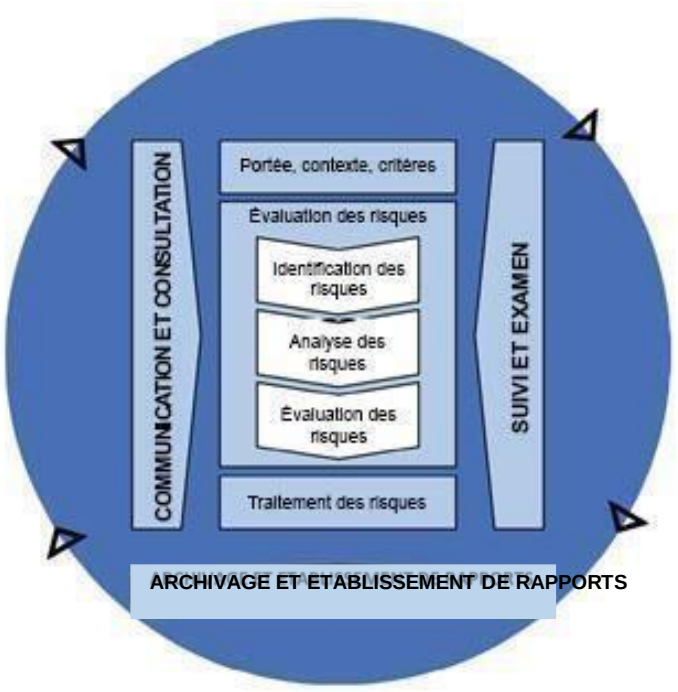
La politique de GRI est le cadre général pour la gestion des risques dans l'organisation. Elle rassemble plusieurs politiques et procédures normatives de l'ONU/du PNUD qui sont appliquées pour gérer des catégories particulières de risques, le cas échéant, notamment :

- Approche harmonisée des transferts en espèces (HACT)
- Évaluations des capacités (des partenaires et du PNUD)
- Politique anti-fraude du PNUD
- Cadre de la criticité des programmes des Nations Unies
- Politique relative à la gestion des risques de sécurité (SRM) des Nations Unies
- Gestion de la continuité des activités
- Politique du PNUD en matière de diligence raisonnable et de partenariats avec le secteur privé
- Assurance qualité du projet/programme
- Normes environnementales et sociales et procédure de détection
- Théorie du changement
- Audits et évaluations
- Politique relative à la fraude et aux pratiques de corruption en matière d'achats
- Stratégie d'approvisionnement et planification des achats

Pour atteindre les objectifs de la politique, la politique de GRI du PNUD repose sur quatre piliers, résumés dans le diagramme suivant :

2. Méthodologie de la GRI

La méthodologie de la GRI comprend six éléments clés conformes à la norme ISO 31000 :2018 : communication et consultation ; établissement du champ d'application, du contexte et des critères ; évaluation des risques ; traitement des risques ; suivi et examen ; et enregistrement et établissement de rapports. Ces étapes s'appliquent à l'ensemble de l'organisation :



a) au niveau du projet (c.-à-d., projets de développement, dispositifs de coopération, services de développement, projets d'efficacité institutionnelle et de développement, projets de coopération multinationale et de coopération Sud-Sud) ;
b) au niveau du programme/de l'unité (c.-à-d., Bureau/programme de pays, Bureaux/programme régionaux, Bureau/programme centraux) ;
c) au niveau de l'entreprise.

2.1 Communication concernant les risques et consultation

La GRI exige une approche inclusive en matière de communication et de consultation avec toutes les parties prenantes concernées, y compris les fonctionnaires chargés des programmes et des opérations, ainsi que les autres parties prenantes concernées (p. ex., système des Nations Unies, partenaires nationaux, experts, donateurs, groupes cibles et personnes concernées par le projet). La communication et la consultation ont lieu à intervalles réguliers/planifiés pour contribuer à l'identification, à l'évaluation, au traitement, au suivi, à l'établissement de rapports et à l'examen des risques.

2.2 Établissement du champ d'application, du contexte et des critères

La politique de GRI du PNUD définit le champ d'application et les critères en matière de gestion cohérente des risques au sein de toute l'organisation. Le goût du risque peut varier au niveau de l'unité/du bureau en fonction du contexte et des objectifs.

L'établissement du contexte nécessite de comprendre le contexte externe et interne pertinent pour la réalisation des objectifs à chaque niveau. Le **contexte externe** comprend, mais sans s'y limiter, les facteurs sociaux, culturels, environnementaux (y compris les risques naturels et le changement climatique), politiques, juridiques, financiers, technologiques, sécuritaires et économiques. Cela implique également de comprendre les parties prenantes externes et leurs relations, perceptions et attentes. De même, le **contexte interne** comprend les objectifs stratégiques, les valeurs, les normes, les ressources disponibles, les processus opérationnels, la culture organisationnelle, les relations avec les parties prenantes internes, les capacités, etc.

2.3 Évaluation des risques

L'évaluation des risques est le processus itératif d'identification, d'analyse et d'évaluation des risques. L'objectif est de fournir suffisamment d'informations à des intervalles appropriés pour des décisions de gestion tenant compte des risques. Des évaluations des risques de haute qualité permettent une meilleure acceptation des occasions de prise de risques (p. ex., l'innovation) tout en garantissant une diligence raisonnable, un traitement, un suivi et un contrôle rigoureux.

Identification des risques

Le **risque** est l'effet de l'incertitude sur les objectifs de l'organisation et de la programmation, qui peuvent être positifs et/ou négatifs. Un risque, lorsqu'il est identifié, peut améliorer, prévenir, dégrader, accélérer ou retarder la réalisation des objectifs. L'identification des risques prend en compte les « événements futurs », leurs causes et leur impact potentiel. Par conséquent, l'identification des risques nécessite

de comprendre le contexte, les schémas des risques historiques et une approche prospective afin de révéler les scénarios futurs et les incertitudes relatives aux objectifs organisationnels et/ou aux résultats de développement.

Les risques potentiels dans toutes les catégories de risque de la GRI (voir l'annexe 2) doivent être pris en compte pour s'assurer que tous les risques pertinents sont identifiés.

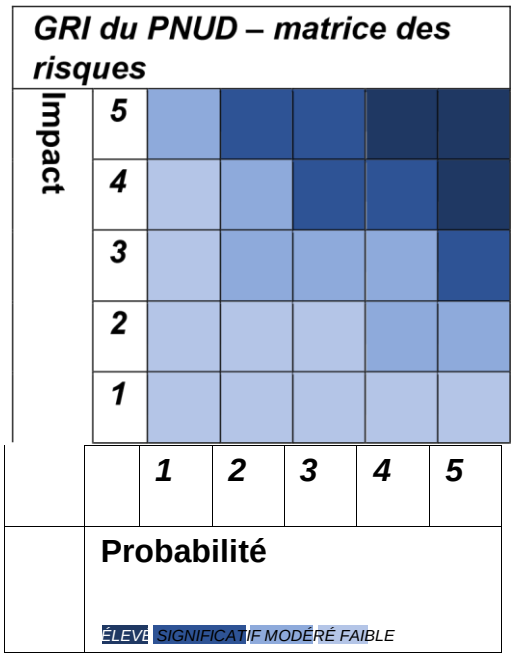
Chaque risque identifié, y compris ceux identifiés par les processus normatifs pertinents énumérés ci-dessus (p. ex., HACT, SESP, évaluation du risque de fraude), est consigné dans le registre des risques et décrit en fonction de la cause, de l'événement/du scénario futur et de l'impact, et est classé dans une catégorie.

Analyse des risques

L'analyse des risques nécessite une évaluation de la **probabilité** d'un risque et de son **impact** potentiel sur les objectifs. Le modèle de critères de la GRI (voir l'annexe 3) définit l'échelle à cinq points utilisés pour déterminer la probabilité et l'impact. Au niveau du programme/de l'unité et de l'entreprise, une analyse plus détaillée des conséquences est appliquée pour déterminer l'impact global. L'apport en capital nécessaire pour absorber les pertes imprévues est défini en fonction des conséquences financières.

Les informations et les preuves disponibles sont prises en compte dans l'évaluation de la probabilité et de l'impact. Le cas échéant, l'analyse des risques comprend l'utilisation d'analyses thématiques pertinentes (p. ex., analyse des risques pour la sécurité, évaluation du risque de fraude, évaluation de l'impact social et environnemental). Au cas où il est difficile d'estimer la probabilité et/ou l'impact et qu'il existe un risque de dommage, une approche préventive est appliquée en estimant le scénario catastrophe afin de garantir que le risque est traité en conséquence et est étroitement surveillé. L'analyse des risques doit être adaptée si davantage d'informations sont disponibles et du moment que ces dernières le sont.

Sur la base de la probabilité et de l'impact, le niveau d'**importance du risque** (élevé, significatif, modéré ou faible) est déterminé à l'aide de la matrice des risques de la GRI présentée ci-dessous.



Les risques de niveau ÉLEVÉ nécessitent une transmission aux échelons supérieurs et une analyse approfondie des risques. Des mécanismes de contrôle des risques supplémentaires doivent être mis en place et les mesures de traitement des risques clairement identifiées, budgétisées et mises en œuvre ; le suivi fréquent ; et les précautions nécessaires pour assurer la sûreté et la sécurité des fonctionnaires et du personnel ne sont pas compromises, et aucune occasion n'est manquée.

Les risques de niveaux SIGNIFICATIF et MODÉRÉ nécessitent une analyse des risques adaptée à la portée et à la nature des risques avec un traitement des risques et des mesures de suivi mises en place et budgétisées. Les risques de niveau SIGNIFICATIF nécessitent une analyse des risques et des plans de gestion des risques plus détaillés.

Les risques de niveau FAIBLE ne nécessitent pas d'analyse ni de traitement supplémentaire.

Évaluation des risques

Sur la base des analyses des risques individuels, ainsi que du goût du risque défini de l'unité/du bureau, une évaluation est effectuée afin de déterminer quels risques peuvent être acceptés et quels risques nécessitent une réponse prioritaire. Les risques qui présentent un potentiel de fraude ou d'utilisation abusive des fonds, de dommages importants pour les personnes ou l'environnement et/ou l'organisation doivent être évités autant que possible ou, autrement, réduits au minimum et atténués. L'évaluation des risques nécessite une prise de décision de la part des responsables hiérarchiques aux niveaux appropriés.

2.4 Traitement des risques

Options de traitement des risques

Pour chaque niveau de risque élevé, significatif ou modéré, une ou plusieurs mesures de traitement des risques doivent être identifiées.

En cas de menace pour les objectifs organisationnels, le traitement des risques peut être de quatre types : **résilier** (chercher à éliminer une activité qui déclenche un tel risque), **transférer** (transfert de propriété et/ou de responsabilité à un tiers), **atténuer** (réduire la probabilité et/ou l'impact du risque en dessous du seuil d'acceptabilité) et **tolérer** (tolérer le niveau de risque).

En cas d'occasion, le traitement des risques peut être de quatre types : **exploiter** (concrétiser l'occasion), **expérimenter** (tester de nouvelles solutions dans des contextes incertains), **améliorer** (augmenter la probabilité ou l'impact en renforçant la condition de déclenchement ou l'exposition croissante) et **accepter** (aucune action proactive).

Appropriation et transmission aux échelons supérieur des risques

Tous les risques sont attribués à un **responsable de la gestion du risque**, la personne qui est responsable en dernier ressort de la gestion appropriée du risque. Chaque mesure de traitement se voit assigner un **responsable du traitement**, la personne responsable de l'exécution du traitement du risque. Le responsable du risque et le responsable du traitement peuvent ou non être la même personne. La propriété est attribuée en fonction du principe de « qui est le plus indiqué » pour assumer la responsabilité de la gestion du risque, en notant qu'il peut être nécessaire que de nombreuses personnes soient impliquées.

Un risque est **transmis aux échelons supérieurs** lorsque les circonstances relatives au traitement lui-même peuvent dépasser le pouvoir/le mandat ou l'expertise du responsable de la gestion du risque. Si une ou plusieurs des conditions de « transmission aux échelons supérieurs » suivantes sont remplies, le propriétaire du risque doit transmettre le risque aux échelons supérieurs :

- Le traitement du risque nécessite des dépenses qui dépassent ce que le propriétaire du risque est autorisé à décider ; et/ou
- Les risques recoupent ou peuvent avoir un impact sur plusieurs bureaux (p. ex., le risque de réputation, les modifications apportées aux politiques de l'entreprise) ; et/ou
- Des réclamations provenant des parties prenantes ont été reçues et le propriétaire du risque ne peut y répondre de manière impartiale et/ou efficace (p. ex., par le mécanisme de réponse aux parties prenantes du PNUD) ; et/ou

- Un grave incident de sécurité s'est produit et a eu une incidence sur le personnel, les installations ou les programmes du PNUD, ou sinon l'environnement de sécurité s'est détérioré et a nécessité des mesures de traitement et/ou des conseils de sécurité supplémentaires ; et/ou • Lorsque le niveau d'importance du risque est jugé élevé.

Lorsque les risques sont transmis aux échelons supérieurs, le propriétaire du risque d'origine doit fournir des informations complètes au gestionnaire destinataire. Le changement de propriété a lieu uniquement après que le gestionnaire destinataire a confirmé qu'il/elle accepte la propriété. Une réponse à la demande de transfert de risque doit être fournie dans les 5 jours ouvrables suivant sa réception, période au cours de laquelle le propriétaire du risque d'origine garde la propriété du risque. La transmission du risque aux échelons supérieurs et le changement de responsable doivent être consignés dans le registre des risques. Au cas où la transmission aux échelons supérieurs serait urgente, le transfert du risque doit être effectué dans les 24 heures et il est permis de communiquer la transmission par téléphone ou par courrier électronique, puis de mettre le registre des risques à jour.

La transmission aux échelons supérieurs se fait par la filière hiérarchique pertinente, c.-à-d., d'un projet au programme au bureau (central/régional) concerné et finalement au niveau de l'entreprise.

2.5 Suivi et examen des risques

Le registre des risques du PNUD constitue une plateforme intégrée pour le suivi de l'ensemble des niveaux et des catégories de risques. **Un suivi et un examen des risques** sont effectués régulièrement pour contribuer aux décisions de gestion, permettant ainsi une gestion adaptative et des changements en cours de route. Les résultats du suivi et de l'examen doivent être enregistrés et signalés comme il convient et utilisés régulièrement pour les décisions, les audits et le rendement de l'organisation en matière de gestion de programmes et de projets. Bien que le suivi des risques soit adapté aux spécificités de chaque risque, le registre des risques doit être mis à jour si de nouvelles informations deviennent disponibles et ont un impact sur l'identification, l'analyse, l'évaluation et les mesures de traitement identifiées. Les occasions de suivi et les menaces en temps réel doivent être prises en compte dans des contextes en évolution rapide afin de fournir un mécanisme d'alerte préventif et de permettre une réponse proactive. En outre, l'état et l'efficacité des mesures de traitement doivent être surveillés en ce qui concerne les niveaux de risque modéré, significatif et élevé, et inclus dans les plans et les budgets de suivi de la gestion des programmes et des projets.

2.6 Enregistrement et établissement de rapports

L'**établissement de rapports sur les risques** garantit que les informations pertinentes sur les risques sont disponibles à tous les niveaux de l'organisation en temps voulu, afin de fournir la base nécessaire à une prise de décision tenant compte des risques. L'établissement de rapports sur les risques doit être réalisé au moins une fois par an. Une fréquence plus élevée de suivi des risques et d'établissement de rapports sur ces derniers liés aux projets peut être nécessaire en fonction du niveau de risque et du contexte (p. ex., des projets d'innovation ou des projets mis en œuvre dans un contexte de risque élevé pour la sécurité, etc.). Les rapports suivants sont requis :

(a) Au niveau de l'entreprise, un rapport annuel au groupe de la direction (GD) et des rapports semestriels au Comité des risques (dans lesquels le deuxième rapport semestriel est remplacé par le rapport annuel) sont nécessaires. Le Comité des risques soumet le rapport annuel sur les risques au GD sur la base d'une analyse stratégique du registre des risques du IWP.

(b) Au niveau du programme/de l'unité, un rapport annuel à travers le rapport annuel axé sur les résultats (RAAR) et un rapport semestriel à travers le registre des risques du IWP. Le deuxième rapport semestriel est remplacé par un rapport annuel. Le registre des risques du IWP se base sur les registres des risques au niveau des projets et une analyse des risques transversaux programmatiques, institutionnels et contextuels. Le gestionnaire de programme examine régulièrement le registre des risques du IWP qui contribue à la prise de décision. La gestion des risques doit se retrouver dans les évaluations à miparcours et finale. Les gestionnaires de programmes doivent également examiner et effectuer le suivi des risques liés aux projets, mais aussi traduire et intégrer les risques pertinents dans le registre des risques du IWP.

(c) Au niveau du projet, le registre des risques du projet est utilisé pour le suivi aussi souvent que nécessaire et au moins une fois par an. Les rapports sur la gestion des risques du projet sont inclus dans les rapports d'avancement du projet (quel que soit le cycle d'établissement de rapports) et envoyés au Comité de pilotage du projet. La gestion des risques doit également être évaluée et incluse dans les rapports d'évaluation de projet à mi-parcours et final.

De plus, l'**établissement de rapports ad hoc** est souvent nécessaire dans les contextes de crise ou pour les risques de haut niveau qui dépendent du temps. Le registre des risques est utilisé pour surveiller ces risques et contribuer aux rapports ad

hoc. Ces rapports doivent inclure une analyse du risque, le traitement/l'état entrepris et un appel à l'action ou une demande d'assistance.

Grâce à son pouvoir statutaire, le PNUD maintient le droit de **divulgation partielle** des risques au public afin d'éviter toute violation de son obligation de confidentialité envers ses bénéficiaires ou de ne pas provoquer de perte de confiance injustifiée envers ses activités ou ses parties prenantes.

3. Système de GRI

Le système de GRI du PNUD est conçu pour aider les fonctionnaires et les partenaires du PNUD à identifier, analyser, surveiller et rapporter les risques existants et nouveaux. Le **registre des risques** est un outil standard de gestion des risques à utiliser pour toutes les catégories de risques (p. ex., financier, programmatique, etc.) et à tous les niveaux de l'organisation. Il ne s'agit pas seulement d'un outil de suivi et d'établissement de rapports, mais également d'un outil de gestion permettant de renforcer la gestion des risques et de contribuer à la prise de décision à tous les niveaux.

Le **registre des risques du projet** reflète les risques auxquels le projet est confronté. Le **registre des risques du programme/de l'unité** reflète les risques significatifs au niveau du projet, considérés comme pertinents pour le programme, les risques transversaux programmatiques et ceux liés aux opérations au niveau de l'unité (ressources humaines, approvisionnement, sécurité, etc.). Le **registre des risques de l'entreprise** reflète les risques au niveau du programme/de l'unité considérés comme critiques pour l'organisation, ainsi que d'autres risques communs à l'ensemble de l'organisation.

4. Gouvernance

4.1 Trois lignes de défense

Les « Trois lignes de défense »[1] soutiennent une gestion des risques plus efficace en introduisant une gouvernance et une surveillance structurées qui clarifient et séparent les rôles et les responsabilités en fonction des éléments suivants :

- Première ligne de défense : fonctions qui possèdent et gèrent les risques ;

[1] *The Three Lines of Defense in Effective Risk Management and Control*, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, janvier 2013) est intégré au modèle de gestion des risques, de surveillance et de responsabilisation des Nations Unies.

- Deuxième ligne de défense : fonctions qui supervisent ou se spécialisent dans la conformité, la gestion des risques ; • Troisième ligne de défense : fonctions qui fournissent une assurance indépendante.

Première ligne de défense

Tout le personnel du PNUD a un rôle à jouer dans la gestion des risques et la première ligne de défense. La responsabilité en matière de GRI repose sur le lien hiérarchique, c.-à-d., le supérieur hiérarchique de chaque unité est responsable de la gestion des risques dans son domaine de responsabilité. Ceci est identifié dans le cadre de responsabilisation du PNUD.

- Au niveau de l'entreprise, le **Groupe de la direction** est responsable de la GRI et veille à ce que les décisions de l'entreprise tiennent compte du risque.

- Au niveau du programme/de l'unité :
    - Les **Directeurs des Bureaux régionaux et centraux** sont responsables de la GRI et de la prise de décisions tenant compte des risques au niveau du Bureau et relèvent de l'Administrateur. Les Directeurs de bureau veillent à ce que les registres de risques des programmes mondiaux/régionaux pertinents soient régulièrement mis à jour, que les risques identifiés soient gérés et transmis au besoin. Les Directeurs des Bureaux ont également la responsabilité de veiller à ce que les bureaux sous leur supervision (p. ex., les bureaux de pays des bureaux régionaux et les bureaux de liaison pour la BERA) tiennent à jour leurs registres des risques, réagissent aux risques de manière appropriée et rendent compte au niveau supérieur en fonction des besoins.

    - Pour les bureaux/programmes de pays, le Représentant **résident/Chef de bureau** est responsable en dernier ressort de la GRI et doit rendre compte au Directeur de Bureau compétent pour s'assurer que le registre des risques de l'unité est surveillé et mis à jour régulièrement, que les risques sont gérés et que tout risque ne pouvant être traité au niveau de l'unité est transmis au bureau compétent.

- Au niveau du projet, la fonction d'**assurance du projet** (p. ex., Administrateur de programme du PNUD) est chargée de veiller à ce que le registre des risques soit régulièrement mis à jour et surveillé pour le projet et que les mesures de traitement des risques soient mises en œuvre.

Deuxième ligne de défense

La deuxième ligne de défense est chargé de la surveillance des risques, du suivi et du soutien technique. Il s'agit d'une fonction essentielle du **Comité des risques** du PNUD, un sous-comité du Groupe de la direction chargé d'établir des rapports sur les risques de l'entreprise au GD deux fois par an et à la demande de celui-ci. Le Comité est présidé par l'Administrateur associé et composé des membres de la haute direction du PNUD. Des experts invités et d'autres représentants concernés peuvent être invités à siéger au Comité. Les principales responsabilités du Comité des risques sont les suivantes :

- Élaborer et proposer la Déclaration relative à l'appétence pour le risque et les principaux indicateurs de risques pour le PNUD ;
- Veiller à ce que le cadre global de gestion des risques soit efficace, pertinent et appliqué au niveau de l'entreprise. ○ Examiner et analyser régulièrement le registre des risques agrégé et les risques transmis afin d'identifier les risques stratégiques et les problèmes qui requièrent l'attention du GD ; et
- Formuler des propositions pour gérer les problèmes/risques transmis (y compris les activités de gestion de la continuité des activités ainsi que de gestion des incidents et des crises).

En outre, les experts techniques compétents (p. ex., sécurité, approvisionnement, finances, opérations, juridique, gestion des programmes et des projets, normes environnementales et sociales) jouent un rôle important dans la deuxième ligne de défense, apportant un contrôle technique, des connaissances et un soutien destiné aux risques de niveau SIGNIFICATIF et ÉLEVÉ.

La deuxième ligne de défense fournit également une surcapacité pour renforcer les Bureaux de pays confrontés à un niveau de risque élevé. Cela comprend la réponse à la crise, les contextes à haut risque, les dommages potentiels ou survenus pour les personnes et/ou l'environnement ainsi que les occasions de prendre des risques et d'innover de façon responsable.

Troisième ligne de défense

La troisième ligne de défense est la fonction d'assurance indépendante et d'audit. Le Bureau de l'audit et des enquêtes (OAI) du PNUD joue ce rôle.

5. Culture de gestion des risques

Le PNUD reconnaît que les mentalités et les comportements d'individus et de groupes au sein de l'organisation jouent un rôle crucial dans l'exécution efficace de la GRI. Une culture mature de gestion des risques se caractérise par les éléments suivants :

- La prise de décision tenant compte des risques à tous les niveaux, notamment la flexibilité pour la gestion adaptative et les changements en cours de route.
- La prise de risque et l'innovation responsables sont couronnées de succès.
- Les « échecs » sont reconnus et pris en compte dans le cadre de la courbe d'apprentissage, en particulier dans des contextes complexes.
- L'apprentissage continu pour renforcer les capacités de gestion des risques.
- Les principales parties prenantes sont impliquées à toutes les étapes du processus de gestion des risques.
- Le défaut d'aborder la gestion des risques uniquement en tant que problème de conformité.
- La communication ouverte sur tous les problèmes de gestion des risques et les enseignements tirés ainsi qu'une culture de « travail à voix haute ».
- La transmission efficace des risques aux échelons supérieurs en cas de besoin.
- Les dotations budgétaires adéquates pour la gestion des risques à tous les niveaux.
- Le personnel du PNUD peut « rester et travailler » à un niveau de risque de sécurité acceptable.

Annexe 1. Termes et définitions

Processus opérationnel. Un processus opérationnel est l'ensemble des activités permettant à une structure organisationnelle d'atteindre ses objectifs.

Conséquence. L'effet pouvant résulter d'un risque s'est-il concrétisé ? Un risque peut avoir plusieurs conséquences, notamment des effets en cascade. Souvent, l'impact total d'un risque dépasse la somme de toutes ses conséquences.

Événement. L'occurrence ou le changement d'un ensemble particulier de circonstances. Un événement peut être une ou plusieurs occurrences, peut avoir plusieurs causes et peut consister en un événement qui ne se produit pas.

Impact. L'ensemble de tous les effets d'un événement ayant une incidence sur les objectifs.

Probabilité. La chance que quelque chose se produise.

Risque. L'effet de l'incertitude sur les objectifs organisationnels, qui pourraient être soit positif soit négatif (ISO 31000 :2018). Le risque est décrit comme un « événement futur », avec ses causes et ses conséquences potentielles. La GRI du PNUD concerne ce qui suit :

- ***Risque institutionnel.*** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver l'efficience et l'efficacité des principales opérations au sein de l'organisation.
- ***Risque programmatique*.** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver la réalisation des objectifs du programme ou du projet.
- ***Risque contextuel*.** Les incertitudes existantes et nouvelles qui pourraient faciliter ou entraver la progression vers les priorités en matière de développement d'une société donnée. La GRI prend en compte le risque contextuel lorsque ces incertitudes externes présentent également des risques institutionnels ou programmatiques. Notez que certains risques contextuels peuvent relever des pratiques de gestion des risques établies et des définitions à prendre en compte (p. ex., pour les risques liés au climat et aux catastrophes).

Goût du risque. Le nombre et le type de risques que les projets, les programmes/unités et le PNUD dans son ensemble sont disposés à prendre pour atteindre leurs objectifs stratégiques à chaque niveau.

Évaluation des risques. Le processus général d'identification, d'analyse et d'évaluation des risques.

Catégories de risque. Un système de classification des risques en fonction de ce que l'organisation fait pour aider à identifier et à suivre systématiquement les risques dans ses principaux domaines de performance.

Transmission des risques aux échelons supérieurs : Le transfert de la propriété du risque au prochain supérieur dans la hiérarchie organisationnelle.

Niveau de risque. L'importance d'un risque exprimé par la combinaison de l'impact et de la probabilité.

Gestion des risques. Activités coordonnées pour diriger et contrôler une organisation par rapport aux risques à tous les niveaux. La gestion des risques consiste à explorer de nouvelles occasions et à éviter des conséquences négatives dans la réalisation de la stratégie du PNUD.

Gestionnaire des risques. Une personne désignée chargée de faciliter et de coordonner la gestion du risque.

Responsable de la gestion du risque. La personne qui est responsable de veiller à ce qu'un risque soit géré de manière appropriée.

Profil des risques. Une description de tout ensemble de risques. L'ensemble de risques peut contenir ceux qui concernent l'ensemble de l'organisation, une partie de l'organisation, du programme ou du projet, ou comme autrement défini.

Registre des risques. Un outil de gestion des risques qui sert à enregistrer tous les risques dans l'ensemble de l'organisation, y compris au niveau du projet, du programme/de l'unité et de l'entreprise. Pour chaque risque identifié, il comprend les informations suivantes : ID de risque, description du risque (cause, événement, conséquences), probabilité, impact, niveau de signification, catégorie de risque, propriétaire du risque, action en faveur du traitement du risque, transmission du risque et état du risque.

Traitement des risques. Une mesure visant à modifier l'exposition au risque afin de fournir une assurance raisonnable contribuant à la réalisation des objectifs. Cela inclut le traitement des risques, qui est une réponse aux événements négatifs, et la gestion des occasions, qui est une réponse aux événements positifs.

Responsable du traitement. La personne qui est responsable de l'exécution du traitement des risques.

Annexe 2 : Catégories de risque en GRI

1.Social et environnemental	2. Financier	3. Opérationnel	4. Organisationnel	5. Politique	2. Réglementaire	7. Stratégique	8. Sûreté et sécurité
1.1. Droits de l'homme 1.2. Genre 1.3. Biodiversité et utilisation des ressources naturelles 1.4. Changement climatique et catastrophe 1.5. Santé et sécurité communautaires 1.6. Conditions/normes de travail 1.7. Héritage culturel 1.8. Droits des peuples autochtones 1.9. Déplacement et réinstallation 1.10. Pollution et utilisation efficace des ressources 1.11. Engagement des parties prenantes 1.12. Exploitation et abus sexuels	2.1. Recouvrement des coûts 2.2. Rapport qualité- prix 2.3. Corruption et fraude 2.4. Fluctuation du taux de crédit, du marché, de la devise 2.5. Livraison	3.1. Harmonisation avec les priorités nationales 3.2. Réactivité aux enseignements tirés et aux évaluations 3.3. Leadership et gestion 3.4. Flexibilité et gestion des occasions 3.5. Potentiel de synergie (lien avec d'autres initiatives, le cas échéant) 3.6. Établissement de rapports et communication 3.7. Partenariat 3.8. Renforcement des capacités des partenaires nationaux 3.9. Engagement des partenaires nationaux dans la prise de décision 3.10. Stratégie de transition et de sortie	4.1. Gouvernance 4.2. Capacité de mise en œuvre 4.3. Modalités de mise en œuvre 4.4. Redevabilité 4.5. Dispositions institutionnelles 4.6. Suivi 4.7. Indépendance et qualité de l'évaluation 4.8. Gestion des connaissances 4.9. Griefs 4.10. Réputation des partenaires du secteur privé 4.11. Ressources humaines 4.12. Disponibilité budgétaire et flux de trésorerie 4.13. Contrôle interne 4.14. Approvisionnement 4.15. Innover, piloter, expérimenter	5.1. Engagement du gouvernement 5.2. Volonté politique 5.3. Instabilité politique 5.4. Changement/renouvellement de gouvernement	6.1. Modifications du cadre réglementaire dans le pays d'opérations 6.2. Modifications du cadre réglementaire international touchant l'ensemble de l'organisation 6.3. Dérogation aux règles et règlements internes du PNUD	7.1. Théorie du changement 7.2. Harmonisation avec les priorités stratégiques du PNUD 7.3. Capacités des partenaires 7.4. Rôles et responsabilités parmi les partenaires 7.5. Code de conduite et d'éthique 7.6. Opinion publique et média 7.7. Coordination et réforme du Système des Nations Unies 7.8. Réputational 7.9. Relations avec les parties prenantes 7.10. Compétition	8.1 Conflit armé 8.2 Terrorisme 8.3 Criminalité 8.4 Troubles civils 8.5 Risques naturels 8.6 Risques d'origine humaine

REMARQUE : Les catégories de risque de la GRI liées aux normes de qualité pour la programmation seront schématisées en conséquence et se retrouveront dans le système de registre des risques/d'AQ

Annexe 3 : Modèle de critères de la GRI – détermination de la probabilité et de l'impact

Détermination de la probabilité (au niveau du projet, du programme/de l'unité, de l'entreprise) :

Probabilité	**Peu probable** **1**	**Faible probabilité** **2**	**Moyennement probable** **3**	**Très probable** **4**	**Prévue** **5**
Description (« Le risque devrait se concrétiser… »)	Tous les 5 ans ou moins **et/ou** très faible chance (< 20 %) de se concrétiser	Tous les 3 à 5 ans **et/ou** faible chance (20 % – 40 %) de se concrétiser	Tous les 1 à 3 ans **et/ou** chance de se concrétiser entre 40 % et 60 %	Une ou deux fois par an **et/ou** grande chance de se concrétiser (60 % – 80 %)	Plusieurs fois par an **et/ou** chance de se concrétiser supérieure à 80 %

Déterminer l'impact :

Au niveau du projet –

Impact	**Négligeable** **1**	**Mineur 2**	**Intermédiaire** **3**	**Étendu** **4**	**Extrême** **5**
	Impact négligeable/nul	5 à 20 % des résultats applicables et prévus ont été impactés, de	20 à 30 % des résultats applicables et prévus ont eu un impact positif ou négatif. Des impacts négatifs potentiels sur les personnes	30 à 50 % des résultats/effets applicables et prévus ont eu un impact positif ou négatif. Impacts	Plus de 50 % des résultats/effets applicables et

Description (« Si le risque se concrétise, ... »)	sur les résultats du projet, positif ou négatif. Impacts négatifs négligeables ou nuls sur les personnes et/ou l'environnement.	manière positive ou négative. Impacts négatifs potentiels sur les personnes et/ou l'environnement très limités et faciles à gérer.	et/ou l'environnement de faible ampleur, limités en importance et en durée, peuvent être évités, gérés ou atténués avec des mesures acceptées.	négatifs potentiels sur les personnes et/ou l'environnement d'ampleur, d'étendue spatiale et de durée moyenne à grande.	prévus ont eu un impact positif ou négatif. Impacts négatifs sur les personnes et/ou l'environnement de grande ampleur, étendue spatiale et/ou durée.

Au niveau du programme/de l'unité et de l'entreprise –

Les analyses suivantes des conséquences potentielles pour l'organisation sont effectuées pour chaque risque. **L'IMPACT global du risque est ensuite déterminé en fonction du niveau d'impact le plus élevé.**

Impact		**Négligeable 1**	**Mineur 2**	**Intermédiaire 3**	**Étendu 4**	**Extrême 5**
	Financier (absolu et relatif)	Plage estimée en USD, 3 chiffres : • Maximum (plus haut niveau d'écart potentiel, +/-) • Probable (*meilleure estimation*) • Minimum (*plus bas niveau d'écart potentiel*, +/-) qui, selon la meilleure estimation, correspond à :				
		<5 % d'écart par rapport au budget applicable	5 à 20 % d'écart par rapport au budget applicable	20 à 30 % d'écart par rapport au budget applicable	30 à 50 % d'écart par rapport au budget applicable	>50 % d'écart par rapport au budget applicable
	Résultats de développement	Impact négligeable/nul sur les résultats/effets, **positif** ou négatif	5 à 20 % des résultats/effets applicables et prévus ont eu un impact positif ou négatif	20 à 30 % des résultats/effets applicables et prévus ont eu un impact positif ou négatif	30 à 50 % des résultats/effets applicables et prévus ont eu un impact positif ou négatif	Plus de 50 % des résultats/effets applicables et prévus ont eu un impact positif ou négatif

Description de la conséquence						
	Opérations	Retard ou accélération des opérations applicables de 1 à 2 jours	Retard ou accélération des opérations applicables 2 à 7 jours	Retard ou accélération des opérations applicables 1 à 4 semaines	Retard ou accélération des opérations applicables pendant un mois ou plus	Changement permanent dans les opérations applicables
	Conformité	Écart négligeable par rapport aux règles et réglementations applicables	Écart modéré par rapport aux règles et réglementations applicables	Écart par rapport aux règles et réglementations applicables	Écart significatif par rapport aux règles et réglementations applicables	Écart majeur par rapport aux règles et règlements applicables
	Sûreté et sécurité	Aucun effet sur le personnel du PNUD et/ou Aucun effet sur les opérations et les programmes du PNUD	Effet légèrement préjudiciable sur le personnel du PNUD et/ou blessures causées directement ou indirectement à la population en général par les actions du PNUD	Effet modérément préjudiciable ou psychologiquement traumatisant et/ou blessures majeures causées directement ou indirectement à la population en général par les actions du PNUD	Effet fatal (individuel ou sur un petit nombre), gravement préjudiciable ou psychologiquement grave et/ou pertes en vies humaines directement ou indirectement dans la population en général par les actions du PNUD	Effet dramatiquement fatal (pertes massives) et/ou pertes en vies humaines directement ou indirectement dans la population en général par les actions du PNUD
	Réputation	Commentaires négatifs ou positifs isolés de parties prenantes externes	Plusieurs commentaires négatifs ou positifs de parties prenantes externes	Rapports/article s négatifs ou positifs dans les médias nationaux, régionaux et/ou internationaux	Rapports/articles négatifs ou positifs dans plusieurs médias nationaux, régionaux et/ou internationaux pendant une semaine ou plus, et/ou les critiques des principales parties prenantes	Rapports/articles négatifs ou positifs dans plusieurs médias nationaux, régionaux et/ou internationaux pour une période d'un mois ou plus, et/ou de vives critiques des principaux acteurs

Avertissement : Ce document a été traduit de l'anglais vers le français. En cas de divergence entre cette traduction et le document anglais original, le document anglais original prévaudra.

Disclaimer : This document was translated from English to French. In the event of any discrepancy between this translation and the original English document, the original English doument shall prevail.