Méthodologie DEMARIS

Démarche de Maîtrise des Risques

Date de mise à jour : 10/06/2010
Version : 2
Auteurs : Pierre CHAMPSAVOIR / Romain ROUSSEAU – Oxéa CONSEIL
Contributeurs : Groupe Projet SIRISBEAC
Validateur : Coordonnateur SIRISBEAC
Destinataire : Correspondants SIRISBEAC

SOMMAIRE

Une démarche inscrite dans les standards internationaux

DEMARIS est le nom de la méthodologie de la BEAC concernant la **démarche de maitrise des risques opérationnels**, qui est implémenté à travers SIRISBEAC. Cette démarche participe à l'amélioration continue de la maitrise des activités de la BEAC, ainsi qu'à la modernisation de ses outils de contrôle interne.

DEMARIS s'appuie sur les exigences de la méthode standard définie par le pilier 1 des **accords Bâle 2**, s'arrimant ainsi à un **référentiel international** pour la gestion des risques au sein des établissements financiers.

Statutairement, la BEAC n'est pas soumise à une obligation de mise en œuvre des accords Bâle 2 en raison de son rôle institutionnel de banque centrale. Cependant, par la mise en œuvre de DEMARIS, **la BEAC inscrit sa gestion dans les meilleurs pratiques internationales** et montre l'exemple pour la sous région.

La méthodologie DEMARIS étant le rouage central d'une **modernisation transverse des outils de pilotage et de contrôle interne**, elle s'inspire aussi d'autres références internationales :

- **Accords Bâle 2**, pour son évaluation qualitative des **risques opérationnels** ;
- **Règlement CRBF 97-02**, pour sa **structure du contrôle interne**, traduite par le règlement COBAC R-2001-07 ;
- **Référentiel COSO**, pour son analyse et son évaluation des **dispositifs de contrôle interne** ;
- **Démarche ISO 9001-2008**, pour son **approche par processus** intégrant la modélisation et les indicateurs de risque et de performance.

Résumé des principaux référentiels internationaux

Accords Bâle 2 : Les normes Bâle 2 (le Nouvel Accord de Bâle) constituent un dispositif prudentiel destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie et les exigences en fonds propres. Les recommandations de Bâle II s'appuient sur trois piliers :

- L'exigence de fonds propres en fonction du ratio de solvabilité McDonough ;
- La procédure de surveillance de la gestion des fonds propres ;
- La discipline du marché instituant la transparence dans la communication des établissements.

CRBF 97-02 : Règlement du Comité de la Réglementation Bancaire et Financière, le CRBF 97-02 institue en France les bonnes pratiques en matière de Contrôle Interne. Il a été récemment amendé pour souligner le rôle de la Gestion des Risques au sein du dispositif de Gouvernance des établissements financiers.

COSO 1 et 2 : Le COSO est un référentiel de contrôle interne défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*, une commission à but non lucratif qui a établit en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer son efficacité. Le référentiel COSO est basé sur les principes de base suivants :

- Le contrôle interne est un processus : il ne se cantonne pas à un recueil de procédures mais nécessite l'implication de tous les acteurs à chaque niveau de l'organisation ;
- Le contrôle interne doit procurer l'assurance raisonnable, mais non absolue, d'un management et d'une direction respectueuse des lois ;
- Le contrôle interne est adapté à la réalisation effective des objectifs de l'établissement.

ISO 9001-2008 : La norme ISO 9001 est relative aux systèmes de gestion de la qualité. La version en vigueur de ISO 9001 est la version datée de novembre 2008. Les exigences y sont relatives à quatre grands domaines :

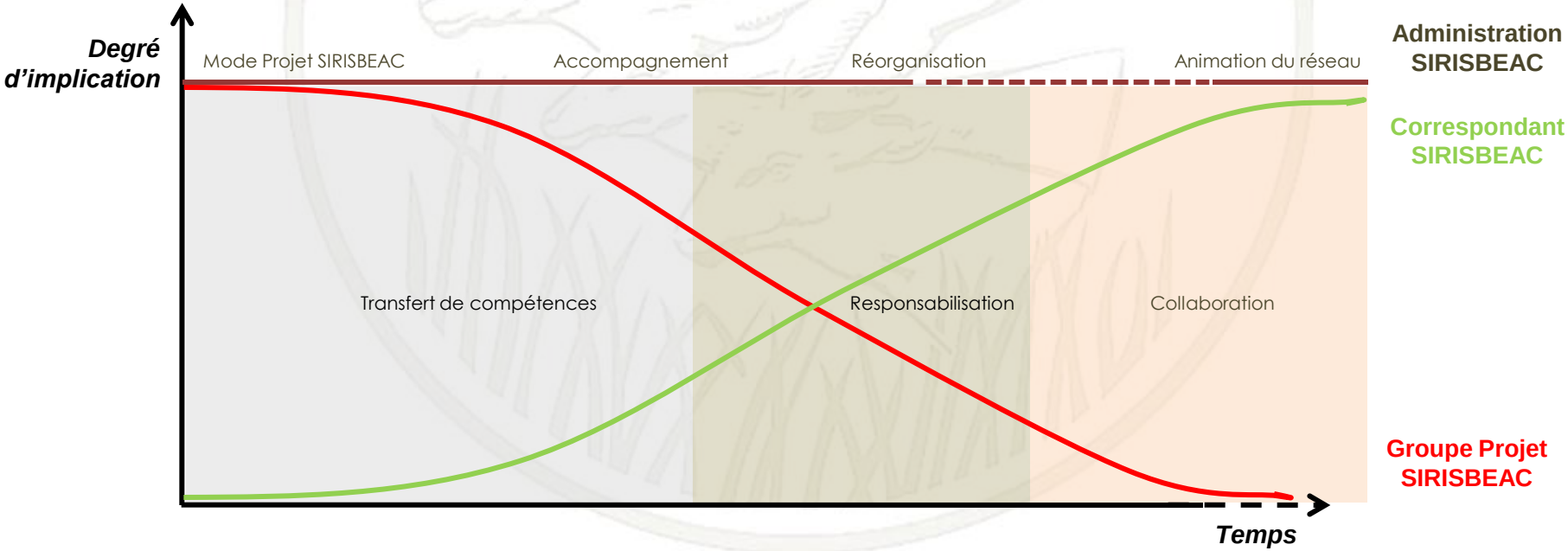
- Responsabilité de la direction en tant que premier acteur et permanent de la démarche ;
- Exigences administratives permettant la sauvegarde des acquis, à travers un système d'information historisé ;
- Exigences relatives à l'identification et à la gestion des processus contribuant à la satisfaction des parties intéressées ;
- Exigences de mesure et enregistrement de la performance à tous les niveaux utiles ainsi que d'engagement d'actions dans le cadre de l'amélioration continue des activités.

Une mise en œuvre en mode projet pour initier le changement

Le Projet SIRISBEAC est en gestation au sein de la BEAC depuis 2004, date à laquelle sous l'impulsion du Gouvernement de la BEAC, la Direction Générale du Contrôle Général a débuté sa sensibilisation à la Gestion des Risques auprès du FMI.

En 2007, le Projet est officialisé sous le nom de SIRISBEAC, et placé sous la coupe de la DGCG en raison de sa participation à venir au dispositif de Gouvernance. Depuis 2007, les équipes en charge du projet ont élaboré la Méthodologie DEMARIS et réalisé un choix d'outil informatique adapté, accompagnées d'experts les assistant dans une démarche progressive de transfert de compétence.

A son tour, l'équipe SIRISBEAC organise depuis 2009 des actions de sensibilisation, puis de transfert compétence et de formation sur les thèmes désormais maitrisés de Gouvernance, Gestion des Risques et Contrôle Interne. Cette conduite du changement permettra de réaliser une responsabilisation progressive de tous les acteurs de la BEAC, fondement même du contrôle interne.



SOMMAIRE

L'organisation de la BEAC, structure de la démarche

La BEAC est organisée en **un ensemble d'unités opérationnelles**, dont on peux distinguer deux grands types :

- Celles relatives aux **Services Centraux** du Siège ;
- Celles relatives aux **Centres** au sein des pays de l'UEMAC.

Selon DEMARIS, les unités opérationnelles des Services Centraux peuvent être rattachée soit au Secrétariat Général soit à une Direction Générale. Elles sont de types Département ou Direction Centrale.

Celles des Centres de l'UEMAC sont rattachées à leur pays de résidence. Elles sont de types Direction Nationales, Agences ou Bureaux. Les quelques Dépôts externalisés sont traités au sein des Directions Nationales des pays de résidence.

Chaque unité opérationnelle est sous la responsabilité d'un Directeur ou d'un Chef de Département.

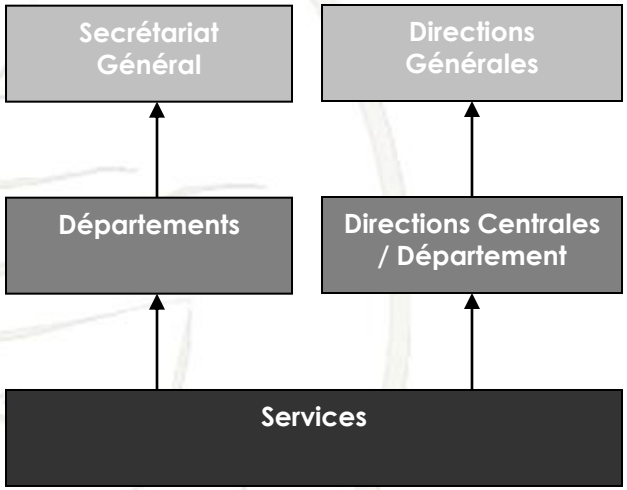
Les unités opérationnel les sont décomposées en service, eux-mêmes sous la responsabilité de Chefs de Services.

Bien que tous les agents de la BEAC soit concerné par la gestion des risques, les responsables identifiés ci-dessus ont un rôle moteur au sein de la méthodologie DEMARIS.

Les Services Centraux

Unités Opérationnelles des Services Centraux

Direction des Etudes
Direction de la Recherche
Direction Relations Internationales
Direction Opérations Financières
Direction Crédit, Marché de Capitaux et Contrôle Bancaire
Direction Formation
Direction Comptabilité
Direction Informatique et Télécommunications
Direction Investissement, Patrimoine et Gestion
Direction Émission Monétaire et Circulation Fiduciaire
Direction Ressources Humaines
Direction Systèmes et Moyens de Paiement
Département Organisation, Affaires Administratives et Réglementation
Département Planification des Moyens Budgétaires et Contrôle de Gestion
Département Affaires Juridiques et Contrats
Département Protocole, Sécurité et Imprimerie
Département Contrôle des Risques et Qualité
Département Etudes et Audit Informatique
Département Contrôle sur Place
Département Contrôle sur Pièces
Bureau Extérieur de Paris
Caisse de Retraite
Cellule Communication
Cellule de Suivi du PSE



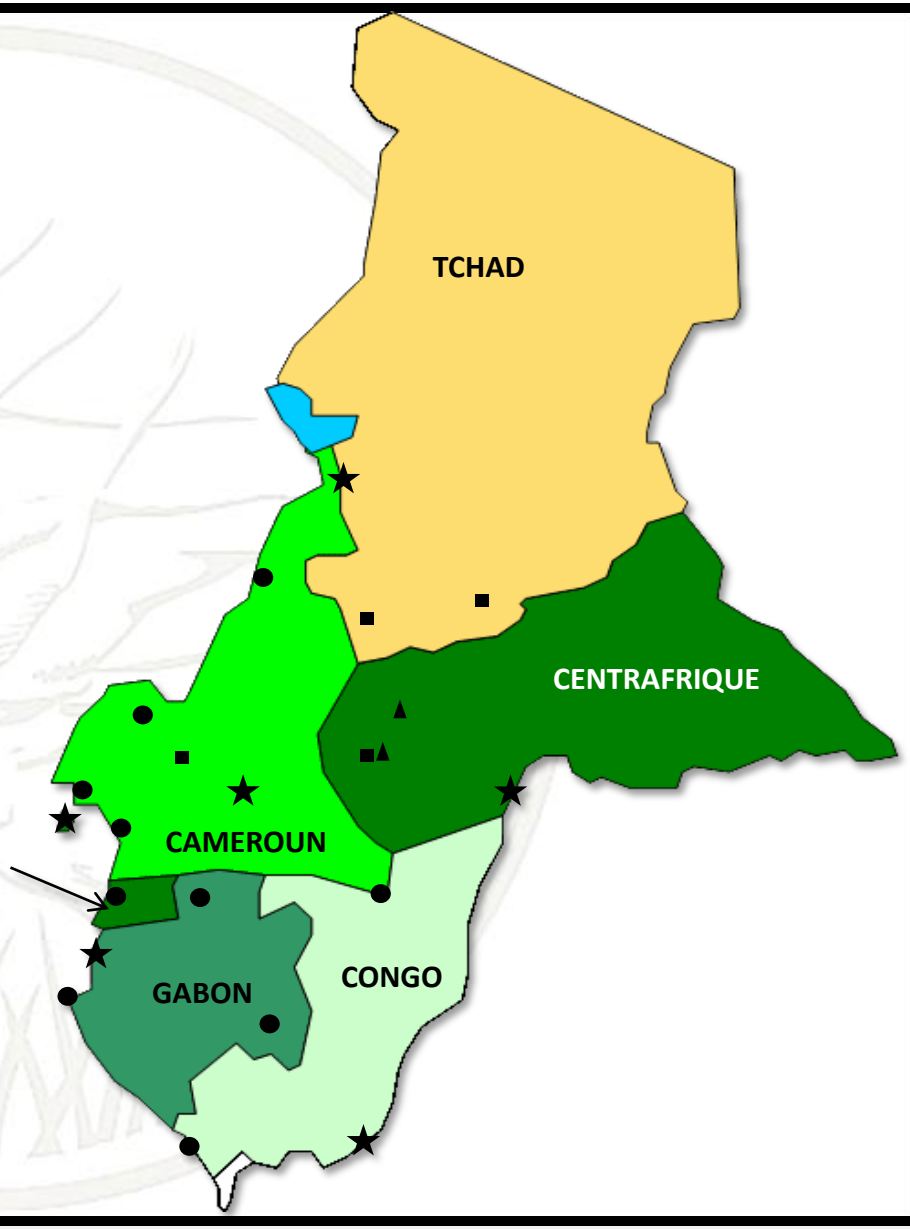
Les Centres de l'UEMAC

Unités Opérationnelles des Services Centraux

Cameroun	Direction Nationale du Cameroun Agence de Douala Agence de Garoua Agence de Bafoussam Agence de Limbe Bureau de Nkongsamba
Centrafrique	Direction Nationale de la Centrafrique (+2 dépôts) Bureau de Berberati
Congo	Direction Nationale du Congo Agence de Pointe Noire Agence de Ouesso
Gabon	Direction Nationale du Gabon Agence de Port Gentil Agence de Franceville Agence de Oyem
Guinée Equatoriale	Direction Nationale de la Guinée Equatoriale Agence de Bata
Tchad	Direction Nationale du Tchad Bureau de Moundou Bureau de Sarh

Légende:

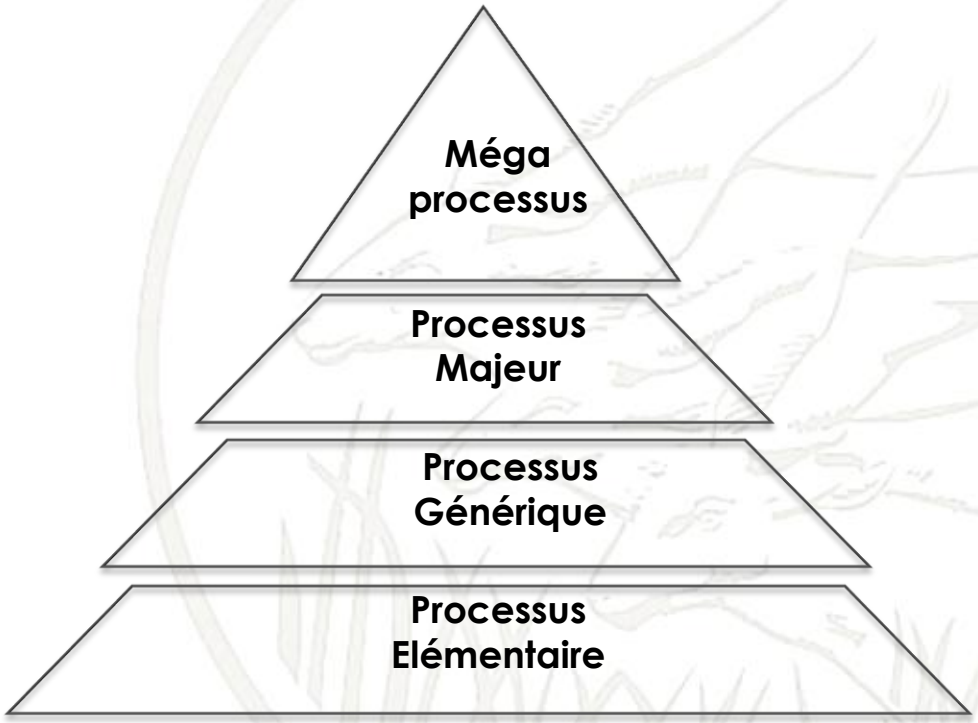
- ★ Direction Nationale
- ● Agence Nationale
- ■ Bureaux
- ▲ Dépôt



SOMMAIRE

Description des Processus Métiers

Le référentiel méthodologique de la BEAC définit quatre niveaux de processus :



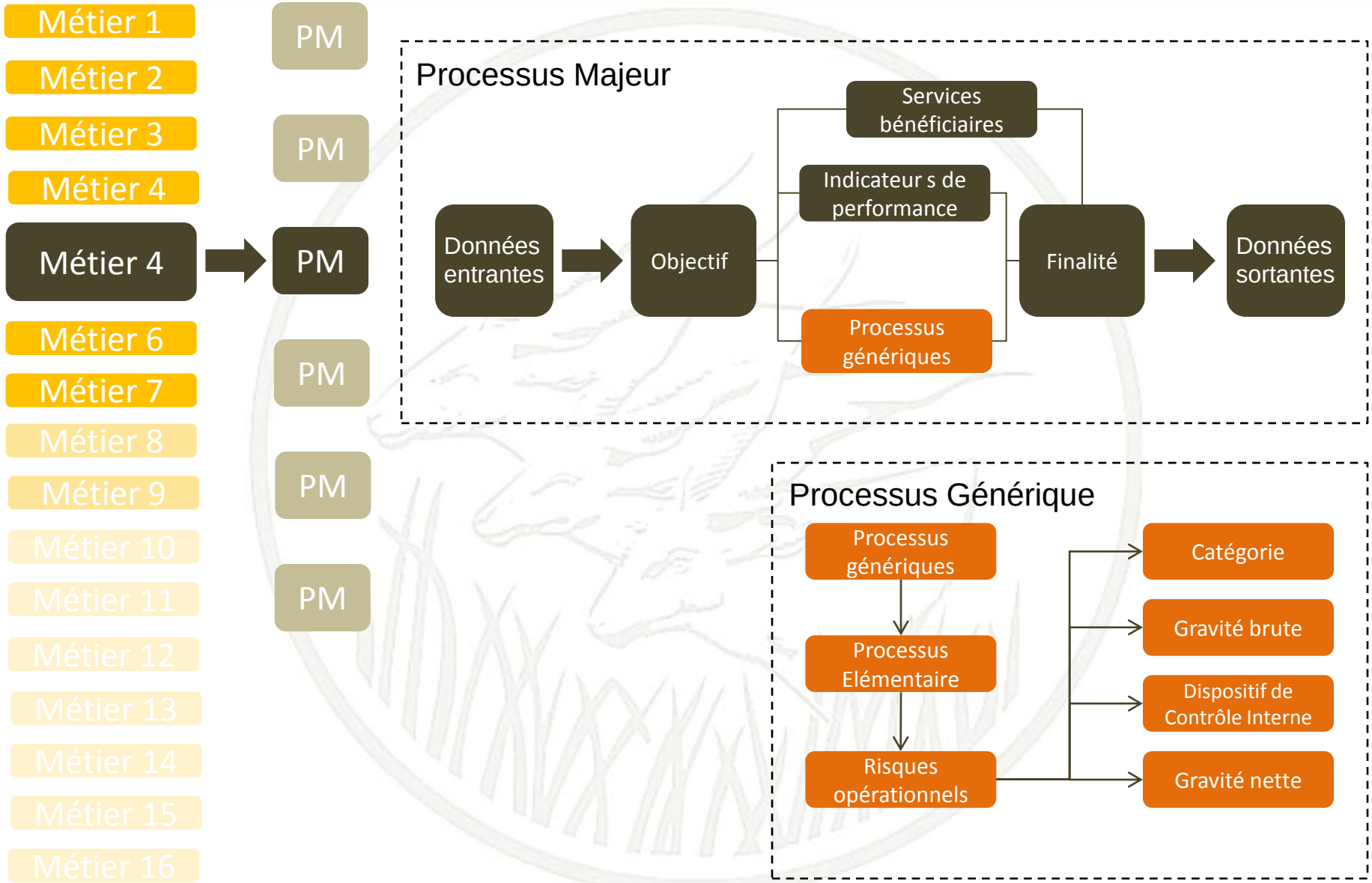
Les Méga Processus représentent l'ensemble des seize (16) **Lignes Métiers de la BEAC** qui lui permettent de réaliser ses objectifs stratégiques.

Les Processus Majeurs correspondent aux activités principales réalisées par les Unités Opérationnelles regroupées dans les Lignes Métiers. Ils sont aussi appelés « **Sous-Métiers** ».

Les Processus Génériques correspondent aux **activités de chaque sous-métiers** réalisées dans les Unités Opérationnelles (Directions Centrales, Départements des Services Centraux, Centres).

Les Processus Elémentaires correspondent aux **activités unitaires** réalisées dans les services des Unités Opérationnelles.

Description des Processus Métiers



SOMMAIRE

Définition du risque opérationnel :

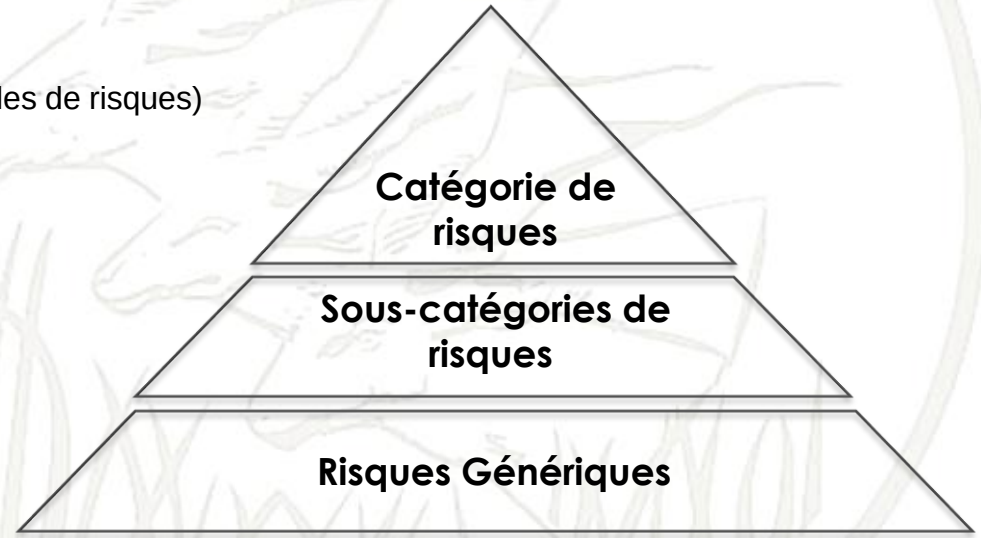
« La BEAC définit le risque comme la possibilité qu'un événement, qu'une action, qu'une situation ou qu'un comportement affecte la réalisation de ses objectifs.»

Il se mesure en terme d'impact et de probabilité. Un risque est rattaché à un processus, de même qu'un processus peut être soumis à un ou plusieurs risques. La typologie générale des risques de la Banque comprend trois niveaux suivants :

Niveau 1 (grandes familles de risques)

Niveau 2

Niveau 3



Dans le cadre de la méthodologie DEMARIS, seuls les risques opérationnels ont été pris en compte. En effet, les risques stratégiques seront suivis par la Cellule de Suivi du PSE et les risques financiers, par la Direction des Opérations Financières dans le cadre des activités de la Salle des Marchés.

Le référentiel de risque

Niveau 1	Niveau 2	Niveau 3
Risques de fraude	Risques liés à la fraude interne	Risque lié à l'implication d'un membre du personnel de la BEAC dans un acte malveillant avec l'intention d'en tirer un profit personnel ou de nuire
		Risque lié au détournement de fonds par un membre du personnel de la BEAC
		Risque lié au vol de fichiers/ données par un membre du personnel de la BEAC
		Risque lié à un conflits d'intérêts, favoritisme ou corruption par un membre du personnel de la BEAC
		Risque lié à la dissimulation d'opérations, falsification de comptes, utilisation de faux documents, usurpation d'identité par un membre du personnel de la BEAC
	Risques liés à la fraude externe	Risque lié au détournement de fonds par une personne externe à la BEAC
		Risque lié au vol de fichiers/ données par une personne externe à la BEAC
		Risque lié à la dissimulation d'opérations, falsification de comptes, utilisation de faux documents, usurpation d'identité par une personne externe à la BEAC
		Risque lié à l'implication d'une personne externe dans un acte malveillant avec une intention manifeste de nuire à la BEAC

Le référentiel de risque

Niveau 1	Niveau 2	Niveau 3
Risques liés aux ressources humaines	Risques liés aux pratiques en matière de ressources humaines	Risque lié à l'inadéquation qualitative des ressources humaines
		Risque lié à l'inadéquation quantitative des ressources humaines
		Risque lié au non respect de la déontologie/ de l'éthique
	Risques liés à l'organisation et au déroulement des activités	Risque lié aux questions sociales
		Risque lié à l'organigramme
		Risque lié à la gestion des carrières
		Risque lié à une erreur ou omission involontaire

Le référentiel de risque

Niveau 1	Niveau 2	Niveau 3
Risques liés aux systèmes d'information et aux technologies	Risques liés aux technologies et systèmes informatiques	Risque lié à la perte d'intégrité ou à l'incohérence des données
		Risque liée à la performance du système d'information (inadaptée ou insuffisante)
		Risque lié à la sécurité du système d'information
		Risque lié à l'indisponibilité du système d'information
	Risques liés à la gestion de l'information	Risque lié à la qualité de l'information
		Risque lié à l'indisponibilité de l'information
		Risque lié à l'absence de piste d'audit
		Risque lié à la communication

Le référentiel de risque

Niveau 1	Niveau 2	Niveau 3
Risques juridiques	Risques contractuels	Risque lié à la mauvaise interprétation des dispositions actuelles ou de l'impossibilité d'exiger l'exécution des contrats entrainant des conséquences néfastes pour la BEAC
		Risque lié au non respect des engagements contractuels vis-à-vis d'un tiers
	Risques de conformité	Risque lié au non-respect des dispositions légales et réglementaires entrainant des conséquences néfastes pour la BEAC
Risques liés à la sécurité physique	Risques liés à la sécurité des personnes	Risque lié à l'insuffisance des dispositifs de sécurité, de prévention, de détection et de protection pouvant mettre en péril la vie des personnes
	Risques liés à la sécurité des biens	Risque lié à l'insuffisance des dispositifs de sécurité, de prévention, de détection et de protection pouvant mettre en péril la sécurité des biens
		Risque lié à un événement d'origine volontaire (terrorisme, vandalisme, incendie volontaire…)
		Risque lié à un événement d'origine non volontaire (catastrophe industrielle, incendie…)

Trois étapes pour l'évaluation des risques

Identification des risques Entretiens avec les experts Métier de la banque

Analyse des risques

Pour l'analyse de la probabilité de survenance et de l'impact, il faut prendre en compte les sources d'informations les plus pertinentes :

- les **données historiques** collectées sur les activités des Unités Opérationnelles ;
- la pratique et **l'expérience des personnes en charge des activités** ;
- les **publications pertinentes** relatives aux domaines à évaluer (rapport d'audit par exemple) ;
- les **recherches et études de marchés** (pour les achats et autres) ;
- les comptes-rendus des **enquêtes d'opinion** ;
- les opinions d'**experts** et de **spécialistes** du domaine concerné par l'évaluation.

Evaluation des risques

Les objectifs définis pour la Banque doivent être pris en compte. On distingue trois niveaux d'évaluations suivantes :

- ***Le Risque Brut (RB)*** **:** appelé également « risque inhérent », est le risque lié à tout processus métier avant la prise en compte du Dispositif de Contrôle Interne. Le principe est que tout risque doit être recensé et évalué même s'il est couvert par un dispositif de contrôle adéquat. Le risque inhérent est évalué en fonction de son impact et de sa probabilité ;

- ***Le Risque Net (RN)*** **:** le risque net se définit comme le risque réévalué après la prise en compte du Dispositif de Contrôle Interne. Le Risque Net traduit l'exposition actuelle et réelle de l'établissement vis-à-vis d'un risque opérationnel ;

- ***Le Risque Cible (RC)*** est le risque souhaité et atteignable, compte tenu des contraintes en matière de gestion. Le niveau du risque cible est une donnée fixée par les dirigeants.

Impacts, probabilité et gravité

Evaluation des impacts et de la probabilité d'un risque opérationnel

Pour l'évaluation du niveau de Gravité d'un risque, la BEAC s'est aligné avec les meilleurs pratiques internationales, conformément à la méthode standard d'évaluation qualitative des risques opérationnels.

Ainsi le risque s'évalue en fonction de son Impact Financier, de son impact d'Image et de sa Probabilité de survenance.

Chacun de ces critères est définit sur une échelle de 5 :
- Très faible ;
- Faible ;
- Moyen ;
- Fort ;
- Très fort.

Ces échelles sont décrites par la suite dans ce chapitre.

Calcul matriciel du niveau de gravité du risque opérationnel

Pour le calcul du niveau de Gravité d'un risque, la BEAC a défini une matrice à deux dimensions, présentée par la suite dans ce chapitre.

Cette matrice définit le niveau de risque selon la formule suivante :

Gravité du risques = (Maximum de l'impact financier et d'image) / (probabilité)

La gravité du risque s'exprime ainsi en 4 zones :
- Risque faible ;
- Risque sensible ;
- Risque majeur ;
- Risque critique.

Echelle de l'impact financier

L'impact financier **:** c'est la conséquence financière directe ou indirecte, immédiate (baisse de revenus ou hausse des coûts).

Echelle de cotation BEAC de l'Impact financier d'un risque opérationnel		
Notation	**Impact**	**Equivalent en Francs CFA**
1	Très faible	De 0 à 4 999 999 XAF
2	Faible	De 5 000 000 à 9 999 999 XAF
3	Moyen	De 10 000 000 à 99 999 999 XAF
4	Fort	De 100 000 000 à 299 999 999 XAF
5	Très Fort	Supérieur à 300 000 000 XAF

Echelle de l'impact d'image

L'impact d'image **:** la conséquence immédiate ou à terme au titre de la dégradation de l'image de la BEAC en interne ou vis-à-vis des tiers externes.

Echelle de cotation BEAC de l'Impact d'Image d'un risque opérationnel		
Notation	**Impact**	**Equivalent illustré**
1	Très faible	• Interruption du service perturbant la bonne exécution d'un processus simple. • Interruption du service bloquant l'exécution d'un processus simple.
2	Faible	• Atteinte mineure de la crédibilité de vis-à-vis de partenaires nationaux ou internationaux. • Détérioration mineure des relations avec les autorités de tutelle et/ou les partenaires majeurs. • Manquement aux missions secondaires de la BEAC. • Conflit avec la profession bancaire.
3	Moyen	• Atteinte notable de la crédibilité de vis-à-vis de partenaires Nationaux ou Internationaux. • Interruption de service bloquant l'exécution d'un processus transversal. • Recours devant des juridictions civiles ou administratives.
4	Fort	• Atteinte grave de la crédibilité de vis-à-vis de partenaires Nationaux ou Internationaux. • Dégradation grave des relations avec les autorités de tutelles et/ou les partenaires majeurs. • Couverture médiatique nationale et internationale négative. • Poursuite devant des juridictions pénales de membres du personnel de la BEAC. • Manquement aux missions fondamentales de la BEAC
5	Très Fort	• Poursuite devant des juridictions pénales à l'encontre des membres du Gouvernement de la BEAC. • Dégradation irréversible des relations entre de et le milieu Bancaire. • Manquement grave aux missions fondamentales de la BEAC. • Dégradation majeure des relations avec les autorités de tutelles et/ou les partenaires majeurs.

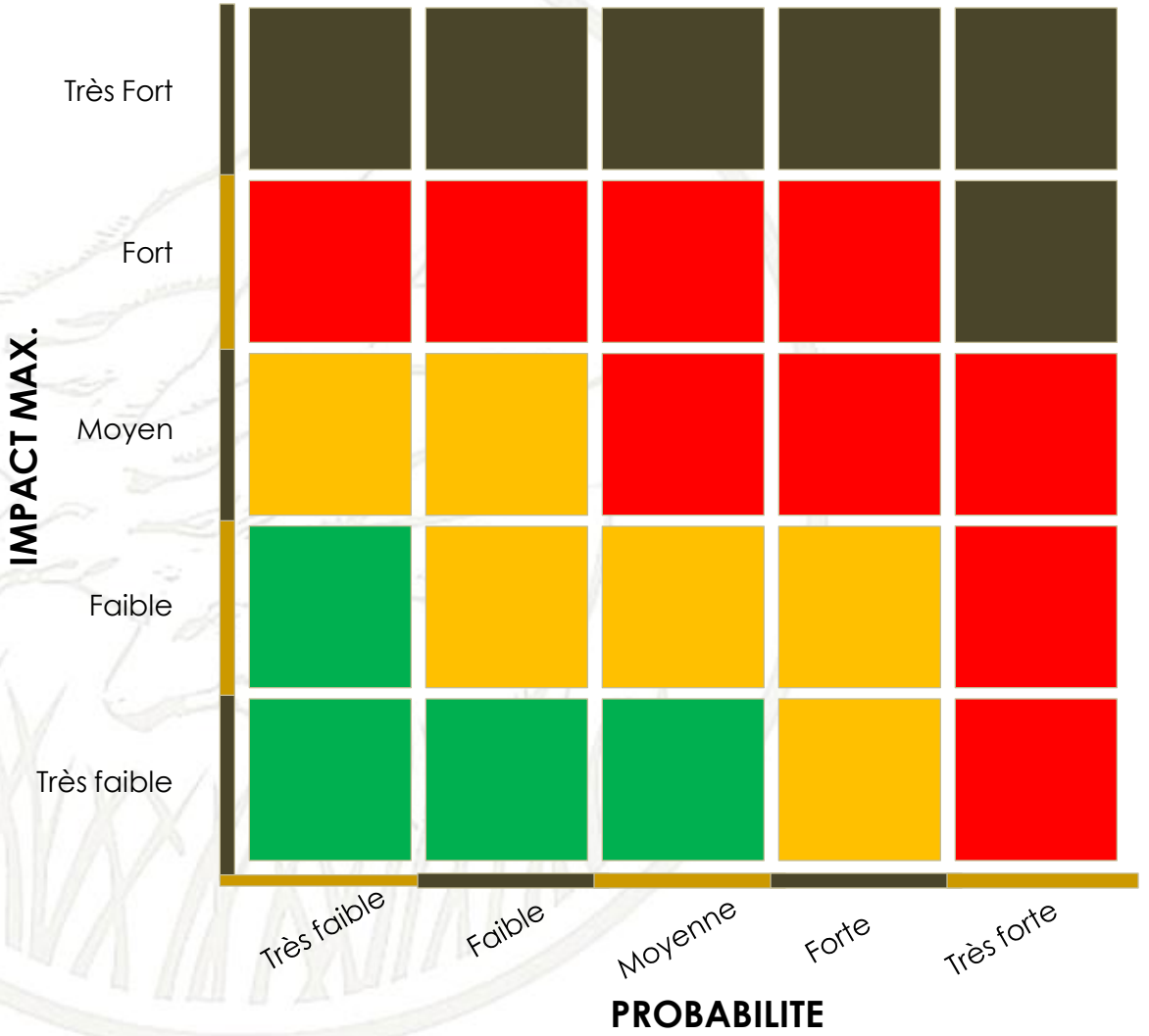
Echelle de la probabilité

La probabilité de survenance : c'est la possibilité plus ou moins forte de subir les conséquences d'un évènement considéré, à tout moment ou dans le temps.

Echelle de cotation BEAC de la probabilité de survenance d'un risque opérationnel			
Notation	**Probabilité**	**En % du volume d'activité**	**En survenance**
1	Très faible	Moins de 20 %	Annuelle
2	Faible	De 20% à 40%	Mensuelle
3	Moyen	De 40% à 60%	Bi- hebdomadaire
4	Fort	De 60% à 80%	Hebdomadaire
5	Très Fort	De 80% à 100%	Quotidienne

La matrice de gravité

Les risques bruts et nets sont évalués en fonction d'une **matrice de gravité commune à toutes les unités opérationnelles** de la BEAC.

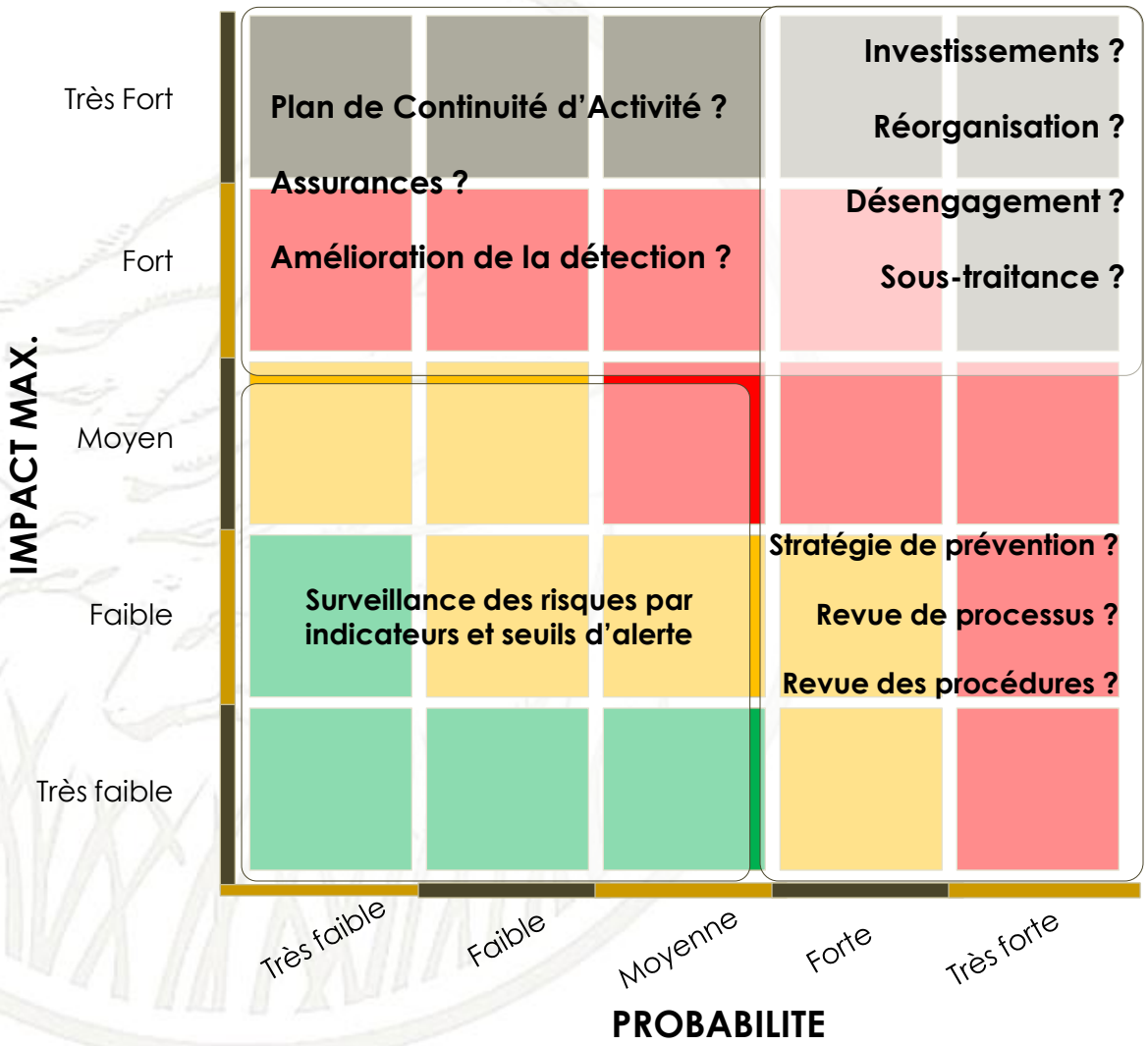


ECHELLE MATRICIELLE DES RISQUES

- Risque critique
- Risque majeur
- Risque sensible
- Risque faible

Exploitation de la matrice de gravité

Cette matrice est **un outil d'analyse puissant** qui vous sera présenté au cours du Projet SIRISBEAC.



ECHELLE MATRICIELLE DES RISQUES

- Risque critique
- Risque majeur
- Risque sensible
- Risque faible

SOMMAIRE

Peu ou pas efficient
Efficient
Très efficient

Définition du Contrôle Interne

« Le Contrôle Interne est un processus mis en œuvre par le Conseil d'Administration, les dirigeants et le personnel d'une organisation destiné à fournir une assurance raisonnable quant à la réalisation des objectifs entrant dans les catégories suivantes :

- ***La réalisation et l'optimisation des opérations ;***
- ***la fiabilité des informations financières ;***
- ***la conformité aux lois et aux réglementations en vigueur. »***

De cette définition, il ressort les trois points suivants :

Le Contrôle Interne est mis en œuvre par l'ensemble des acteurs travaillant dans la Banque ;

Il ne concerne pas seulement le monde des entreprises, mais toutes les organisations ;

L'assurance raisonnable signifie que le Contrôle Interne n'est pas une solution magique permettant de travailler de façon « parfaite », c'est simplement un moyen de mieux faire.

Les six catégories de Dispositifs de Contrôle Interne

Les éléments constitutifs des Dispositifs de Contrôle Interne sont les suivants :

Objectifs :

- Sécurité des Actifs
- Qualité de l'Information
- Respect des Directives
- Optimisation des Ressources disponibles

Moyens :

- Humains
- Financiers
- Techniques

Système d'Information et de Pilotage :

- Données applicables à toutes les fonctions
- Données fiables et auditables
- Données exhaustives
- Données disponibles
- Données utiles et pertinentes

Organisation :

- Organigramme formalisé
- Description de postes précise
- Séparation des tâches et des pouvoirs

Méthodes, procédures et modes opératoires :

- Définis et formalisés
- Connus et partagés

Supervision :

- Rôle d'assistance opérationnelle
- Rôle de gratification des travaux réalisés
- Rôle de vérification et de contrôle

Concepts fondamentaux sur l'évaluation des dispositifs de contrôle interne :

- Un dispositif de contrôle interne est **évalué par rapport à un risque**, et s'applique au sein d'un processus élémentaire associé à ce risque.
- Ces dispositifs peuvent être définis comme les **éléments « mis en œuvre afin de fournir une assurance raisonnable quant à la réalisation des objectifs, principalement sur la réalisation et l'optimisation des opérations, la fiabilité des informations financières enregistrées et la conformité aux lois et réglementations en vigueur »**.
- L'efficience d'un dispositif de contrôle interne est **évaluée en fonction de deux critères** :

Son adéquation, c'est-à-dire la conception globale du dispositif par rapport au risque à couvrir ;

Sa performance, c'est-à-dire sa mise en œuvre concrète par les équipes en fonction de l'activité et des moyens disponibles.

Les trois principes à respecter

L'adaptation :

Il n' y a pas de modèle unique qui pourrait servir de référentiel pour tous. La diversité des organisations est aussi grande que peut l'être la diversité des entreprises (taille, nature d'activité, objectifs, environnement, structure juridique, etc.). Mais le principe essentiel est que l'organisation doit être adaptée à la culture, à l'environnement, à l'activité, etc.

L'objectivité :

Une organisation objective est celle qui n'est pas construite en fonction des hommes. Ce principe consacre la permanence relative dans la mesure où une mutation ou un départ ne doit pas à chaque fois remettre en cause l'organisation existante.

La sécurité ou la séparation des tâches :

S'organiser avec le maximum de sécurité, c'est répartir les tâches de telle façon que certaines d'entre elles, fondamentalement incompatibles, ne puissent être exercées par une seule et même personne. Le principe de la séparation des tâches répond donc à cette préoccupation.

Trois fonctions fondamentales sont incompatibles dans une organisation : les mettre en une seule main, ou même deux d'entre elles, c'est prendre des risques importants avec la sécurité des actifs. Ces trois fonctions sont :

- la fonction d'autorisation (ou décision) ;
- la fonction d'enregistrement comptable ;
- la fonction financière.

SOMMAIRE

Le risque Cible

Vision du Gouvernement de la BEAC

Risque Cible de la Méthodologie DEMARIS

Précision opérationnelle

Définition de la tolérance par catégorie de risques traduisant l'exigence d'amélioration continue de ma maitrise des activités

Définition du risque cible par catégorie de risques traduisant les priorités données au contrôle interne

Identification des processus majeurs traduisant les orientations du Gouvernement de la Banque

Décision du Gouvernement de la Banque et du Comité d'Audit du Conseil d'Administration concernant la stratégie de contrôle interne de la BEAC

Traduction Tactique

SOMMAIRE

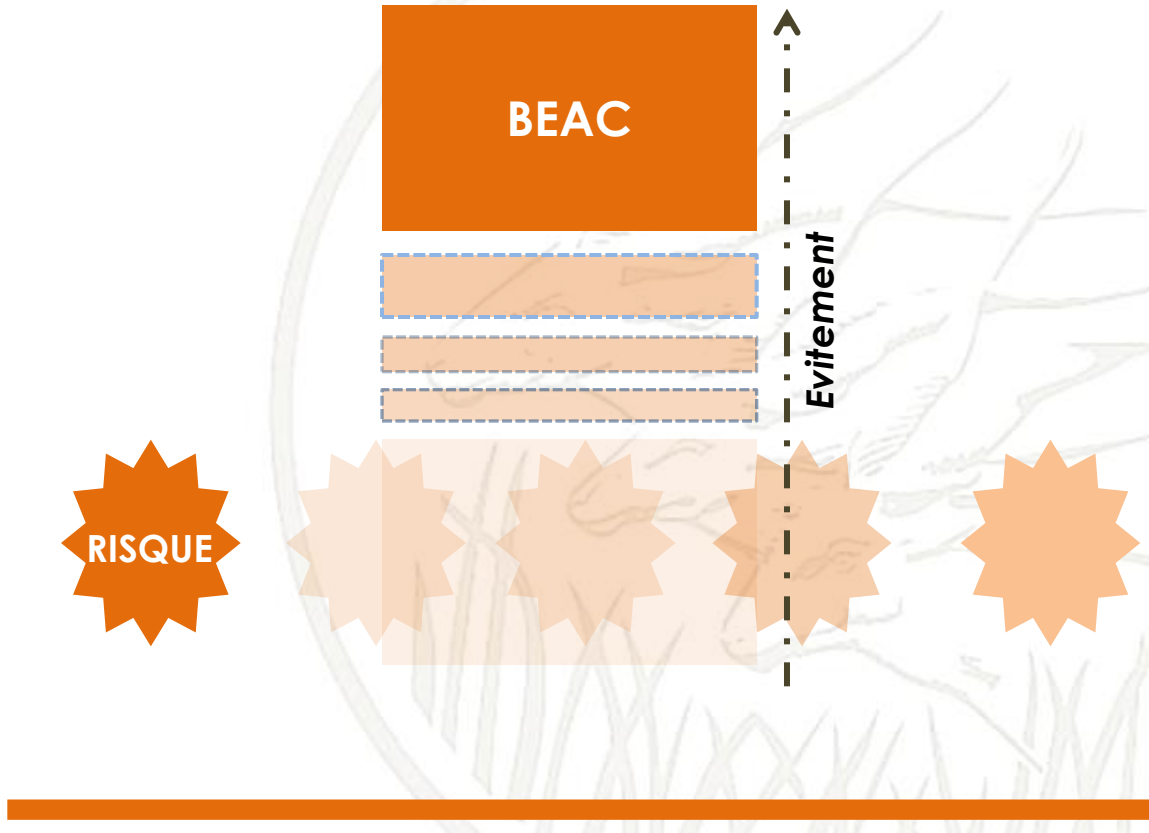
Le traitement des risques

Une fois le risque identifié, il peut être traité de plusieurs façons, cela dépend des composantes du risque, de la stratégie de l'organisation, de ses objectifs opérationnels.

Voici les différents modes de traitement des risques :

- L'évitement ;
- La réduction ;
- La mutualisation ;
- L'acceptation ;
- Le financement ;

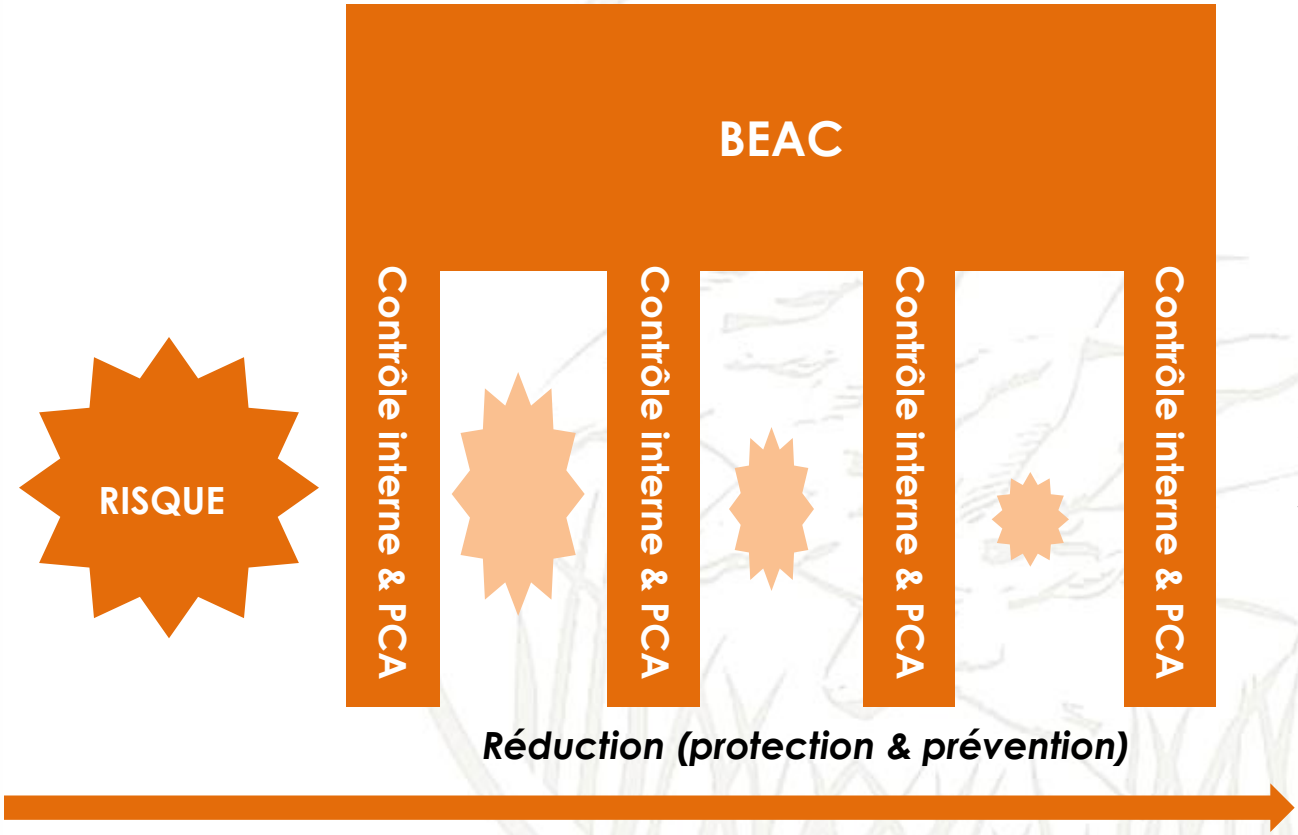
L'évitement



« Stratégie visant à ne pas prendre le risque. Il est assez rarement utilisé dans le monde bancaire mise à part lors d'une sortie d'un marché quelconque. »

Par exemple : En France, ce fut le cas pour le CIC qui après une perte significative sur les marché a décidé d'arrêter définitivement son activité de marché pour compte propre.

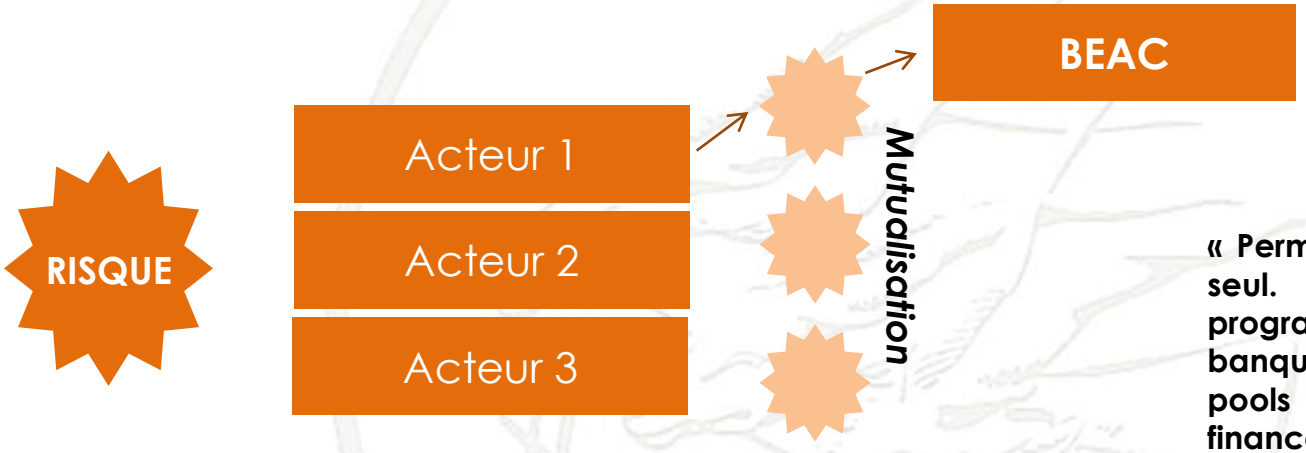
La réduction



« La réduction du risque se fait par des mesures de prévention permettant de jouer sur la fréquence c'est-à-dire le nombre d'occurrence, et des mesures de protection permettant de limiter l'impact. »

Par exemple : Lorsque je met en place un PCA, c'est une mesure de protection. Lorsque je met en place un contrôle bloquant dans un système, c'est une mesure de prévention. Lorsque je vérifie tous les dossiers supérieurs à 1 Millions de CFA, c'est à la fois une mesure de prévention et de protection (je limite le nombre d'erreur sur des opérations de gros montants).

La mutualisation



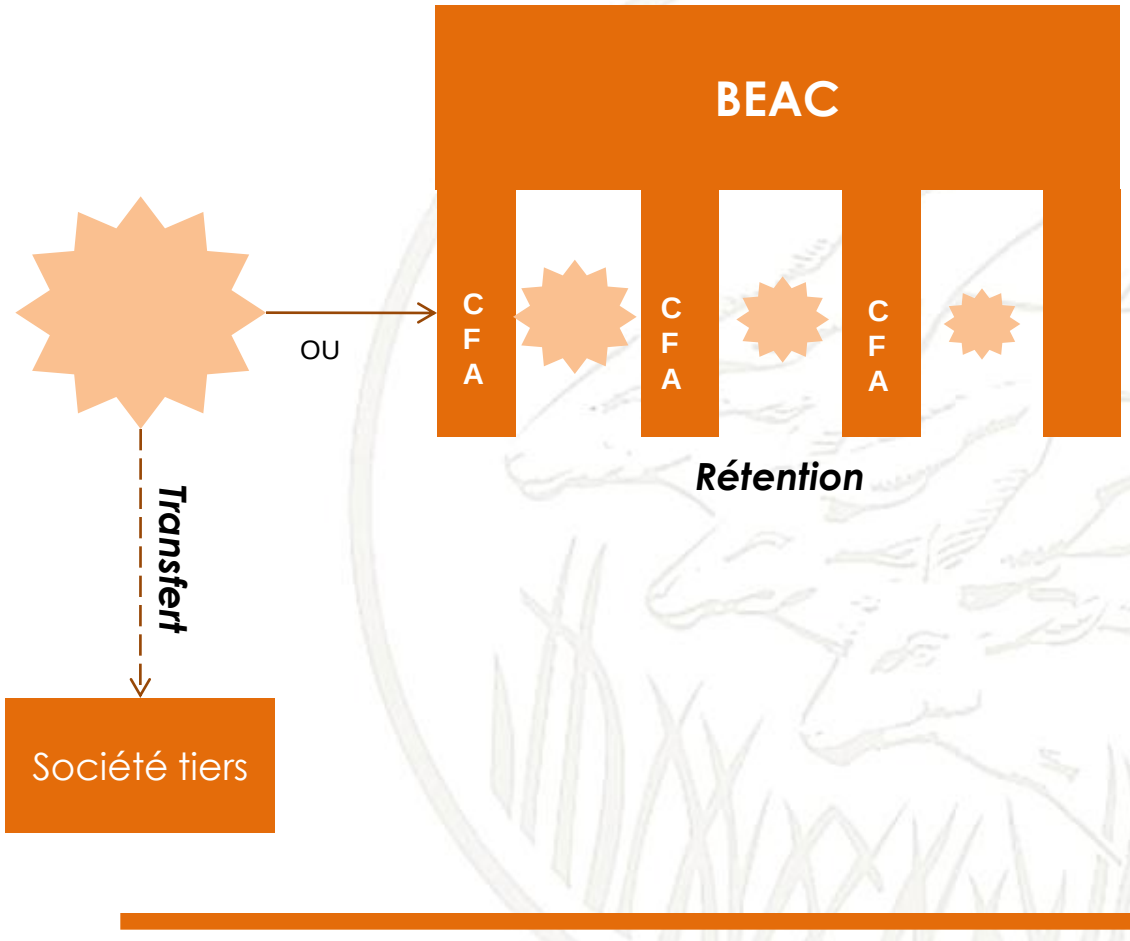
« Permet de ne pas assurer le risque seul. Concerne davantage des programmes d'investissement. Les banques sont amenées à créer des pools bancaires pour des financements de montant élevé afin de prendre qu'une partie du risque global. »

L'acceptation

« C'est le fait d'accepter le risque en l'état et de rien faire. C'est une décision stratégique qui doit se faire en toute connaissance de cause sur les risques sous-jacents. »

Par exemple : Une entreprise peut accepter le lancement d'un produit en l'état malgré les risques car la concurrence à déjà lancé les siens.

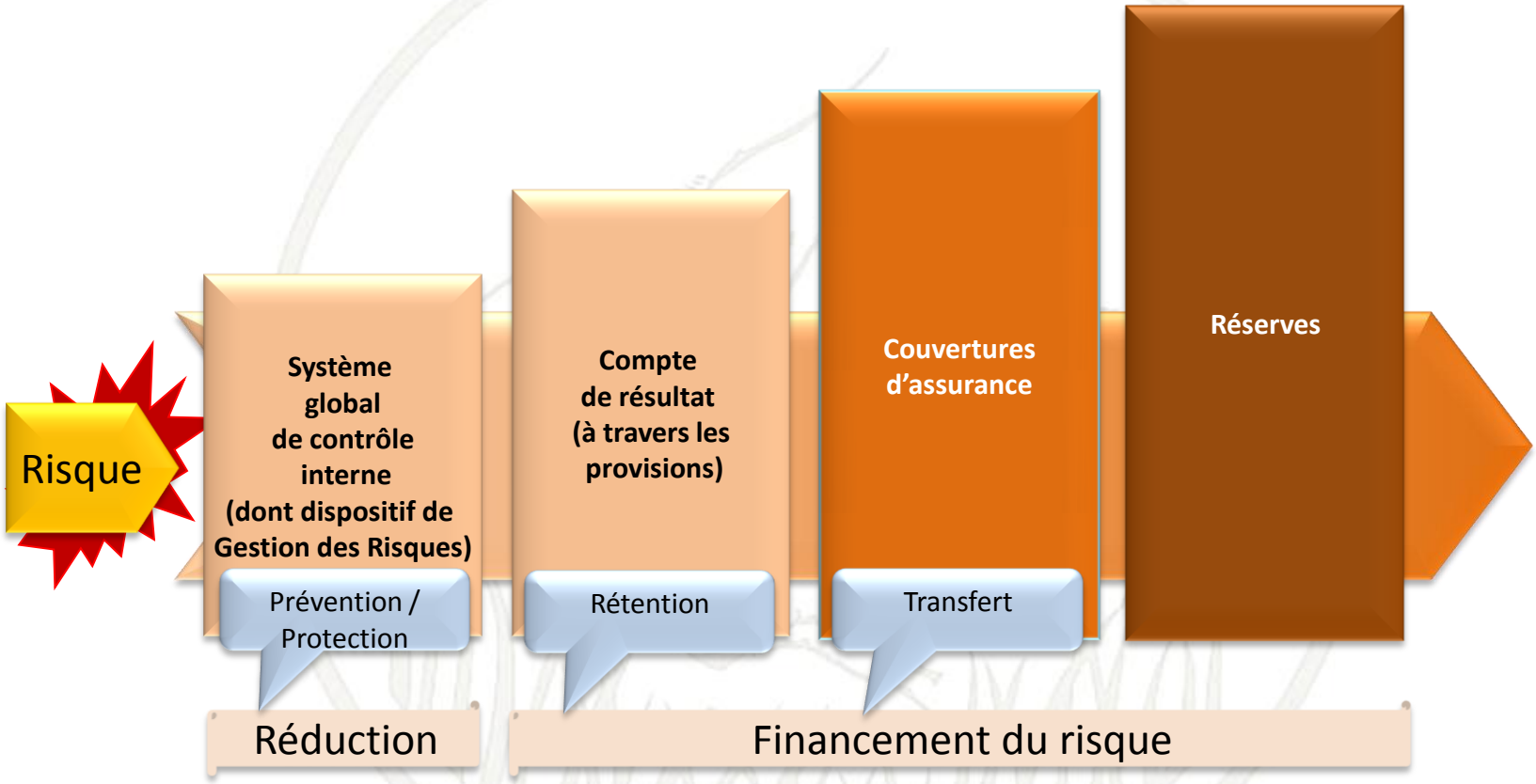
Le financement



« C'est le fait de financer les conséquences du risque soit même à travers ses provisions comptables, c'est la rétention ; ou d'en transférer le financement auprès d'un tiers à travers les politique d'assurance, c'est le transfert du risque. »

Par exemple : Les banques peuvent via la tarification des cartes de paiement financer directement le risque de fraude, ce qui est généralement fait, mais elles pourraient de même solliciter une police d'assurance pour couvrir ce risque.

La cohérence d'ensemble du traitement des risques



SOMMAIRE

Les acteurs de la filière Opérations

Le Gouvernement de la Banque

Les principales fonctions sont :

• Décide de la politique de prévention et de maîtrise des risques de la Banque ;
• Préside le Comité Central de Gestion des Risques de la BEAC où sont exposés les conclusions des Risk-Managers Métiers et Nationaux, et où est décidée la politique de prévention et de maîtrise des risques opérationnels de la BEAC en fonction des objectifs stratégiques ;
• Valide le plan tactique de risques cibles proposé le DCRQ en fonction de la politique de prévention et de maîtrise des risques opérationnels de la BEAC.

Responsable d'Unité Opérationnelle :

• Est identifié par Unité Opérationnelle (Direction, Département ou Centre) ;

Les principales fonctions sont :

•S'assure de la maîtrise des risques opérationnels sur son périmètre :
  •Par métier de manière transverse sur l'ensemble des Centres pour les Responsables Métiers de la Banque;
  •Par pays pour les responsables nationaux des Directions Nationales ;
  •Par centre pour les responsables locaux des Agences et Bureaux.
•Préside les Réunions et Comités de Gestion des Risques sur son périmètre, où sont exposées les conclusions des Risk-Managers et où sont décidés les plans d'action à mettre en œuvre ;
•Est l'ultime validation pour l'enregistrement et le traitement d'un incident sur son périmètre local (Direction, Agence ou Bureau) ;
•Relaie la politique de gestion des risques décidée par le Gouvernement de la Banque, définit et supervise les plans d'action permettant d'atteindre les niveaux de risques cibles sur les processus génériques de son périmètre.

Les acteurs de la filière Opérations

Responsable Opérationnel (RO) :

- Est identifié par Processus Générique pour chaque Unité Opérationnelle ;
- Est responsable d'un ou plusieurs Processus Générique(s) dans son Unité Opérationnelle ;

Les principales fonctions sont :

•Participe à la mise à jour des processus élémentaires sur son périmètre ;
•Identifie, en collaboration avec le Risk-Manager Assistant ou Correspondant de son Unité Opérationnelle, les Risques Génériques et les Dispositifs de Contrôle Interne déployés sur les Processus Elémentaires de son périmètre ;
•Valide l'évaluation des risques opérationnels proposée par le RMA ou le RMC de son Unité Opérationnelle ;
•Déclare et évalue les incidents sur son périmètre ;
•Valide les incidents déclarés par les RM, R0, RMA, RMC, AO ou AGR sur son périmètre ;
•Met en œuvre les actions qui lui sont allouées dans le cadre des plans d'action décidés par en Réunions ou Comités de Gestion des Risques ;
•Supervise le travail des AO et rapporte ses conclusions au RUO.

Assistant Opérationnel (AO) :

- Est identifié par rapport à son Responsable Opérationnel au sein d'une Unité Opérationnelle ;

Les principales fonctions sont :

•Assiste le Responsable Opérationnel dans la mise à jour des Processus Elémentaires sur son périmètre ;
•Assiste le Responsable Opérationnel dans l'identification des risques opérationnels et des dispositifs de contrôle interne sur son périmètre ;
•Déclare et évalue les incidents sur son périmètre ;
•Assiste le Responsable Opérationnel dans la mise en œuvre des actions dans le cadre des plans d'action décidés par en Réunions ou Comités de Gestion des Risques.

Les acteurs de la filière Gestion des risques

Risk-Manager (RM) :

• Est identifié par Métier ou par Pays ;

Les principales fonctions sont :

•Organise et anime le dispositif de gestion des risques opérationnels sur son périmètre (métier ou pays) ;
• Supervise les travaux de son RMA et de ses RMC sur l'identification et l'évaluation des risques opérationnels ;
•Est informé de la création d'un nouveau risque opérationnel sur son périmètre ;
•Valide les évaluations finales des risques opérationnels sur son périmètre ;
•Valide les déclarations et les évaluations d'incidents proposées par les Responsables Opérationnels ;
•Analyse les données consolidées sur son périmètre (Métier ou Pays), et apporte ses préconisations sur les plans d'action à mettre en œuvre pour améliorer la maîtrise des activités et les dispositifs de contrôle interne ;
• Rapporte à l'organe central de prévention des risques de la BEAC et aux Réunions et Comités de Gestion des Risques.

Risk Manager Assistant (RMA) :

• Est identifié par Unité Opérationnelle ;

Les principales fonctions sont :

•Assiste le RM de son Métier ou Pays dans sa supervision des travaux des RMC et dans ses analyses et consolidations des données relatives aux risques opérationnels ;
•Est garant du dynamisme opérationnel du dispositif de gestion des risques, dont il est le représentant et principal référent dans un métier ou un Pays ;
•Identifie et évalue les risques opérationnels, en collaboration avec les RO, et incidents sur son périmètre local (direction ou département) ;
•Supervise et valide les travaux de l'AGR sous sa responsabilité ;
•Préconise et enregistre les plans d'action à mettre en œuvre pour améliorer la maîtrise des activités et l'efficience des dispositifs de contrôle interne ;
•Rapporte au RM en charge de son Unité opérationnelle et participe aux Réunions et Comités de Gestion des Risques.

Les acteurs de la filière Gestion des risques

Risk Manager Correspondant (RMC) :

• Est garant du dynamisme du dispositif de gestion des risques, dont il est le représentant et principal référent local ;

Les principales fonctions sont :

•Identifie et évalue les risques, en collaboration avec les RO, et incidents sur son périmètre ;
•Supervise et valide les travaux de l'AGR sous sa responsabilité ;
•Préconise et enregistre les plans d'action à mettre en œuvre pour améliorer la maîtrise des activités et les dispositifs de contrôle interne ;
• Rapporte au RMA et RM en charge de son Unité Opérationnelle ainsi qu'aux Réunions de Gestion des Risques de son périmètre local.

Assistant Gestion des Risques (AGR) :

Les principales fonctions sont :

•Assiste le RMA ou le RMC dans la réalisation des travaux relatifs au dispositif de gestion des risques opérationnels ;
•Peut identifier et évaluer les risques par délégation du RMA ou RMC en cas d'indisponibilité de celui-ci ;
•Identifie et évalue les incidents sur son périmètre local.

Les acteurs de la filière Contrôle et Administration

L'administrateur fonctionnel SIRISBEAC :

- Est identifié pour l'ensemble de l'application SIRISBEAC ;

Les principales fonctions sont :

- Gère en central tout ce qui a trait aux utilisateurs :
  - création, modification d'un utilisateur ;
  - modification de l'allocation des profils ;
  - création, modification des habilitations relatives aux différents profils ;
- Création et maintenance des référentiels de référence :
  - Unités Opérationnelles ;
  - Processus ;
  - Risques ;
  - Indicateurs.

Création et mise à jour des référentiels de processus locaux instanciés.

L'administrateur technique SIRISBEAC :

- Est identifié pour l'ensemble de l'application SIRISBEAC ;

Les principales fonctions sont :

- Gère en central tout ce qui a l'évolution de l'application :
  - Création, modification d'un champ ou d'un écran ;
  - Modification des règles de gestion ;
  - Importation et exportation de grand volume de données par création de template.
- Gère la maintenance technique de l'application :
  - Installation des modules ;
  - Maintenance et installation des patchs évolutifs.

Le responsable Rapports SIRISBEAC :

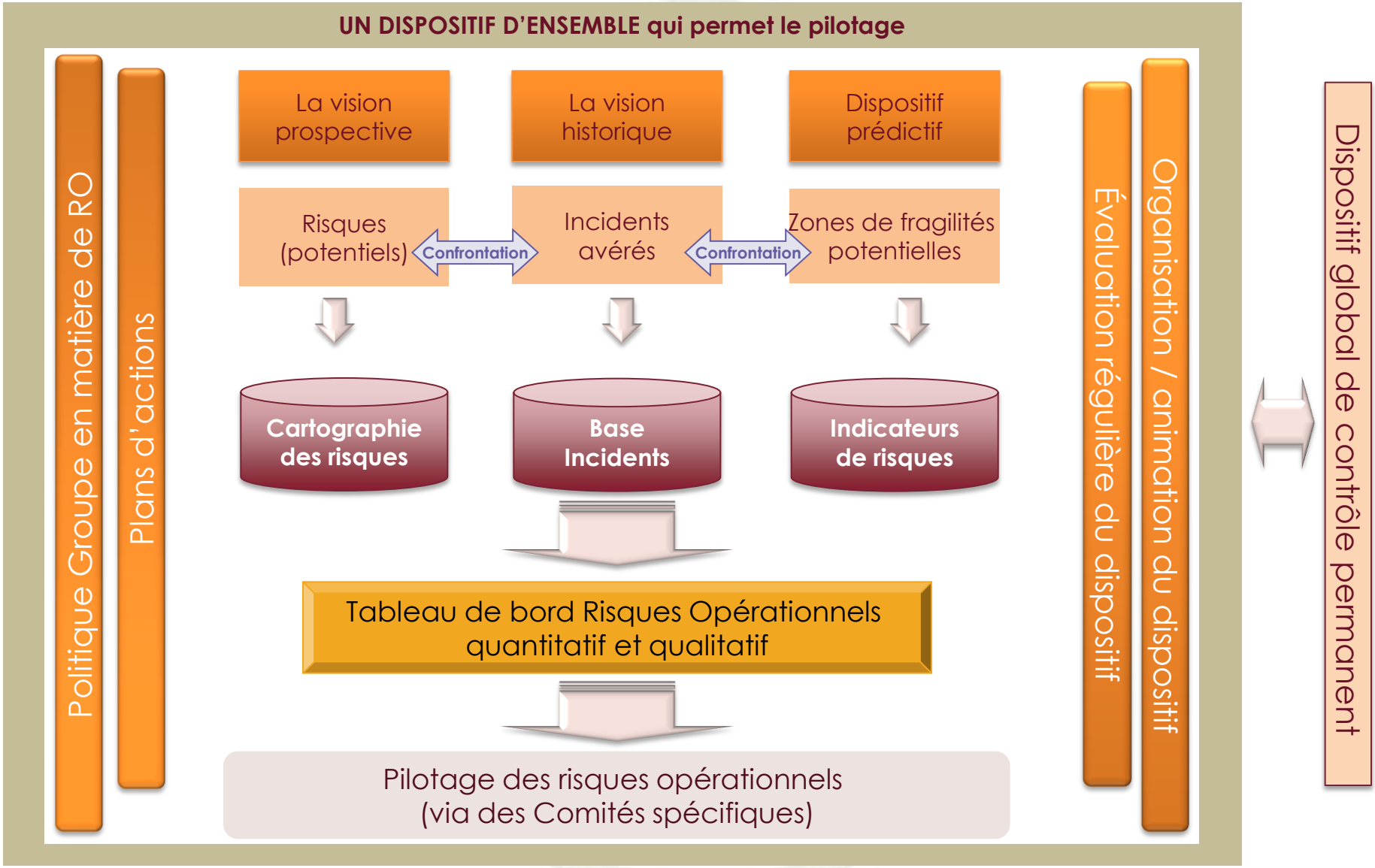
- Est identifié pour l'ensemble de l'application SIRISBEAC ;

Les principales fonctions sont :

- Gère en central tout ce qui a trait aux rapports :
  - Création de nouveaux rapports
  - Modification ou correction d'un rapport existant.

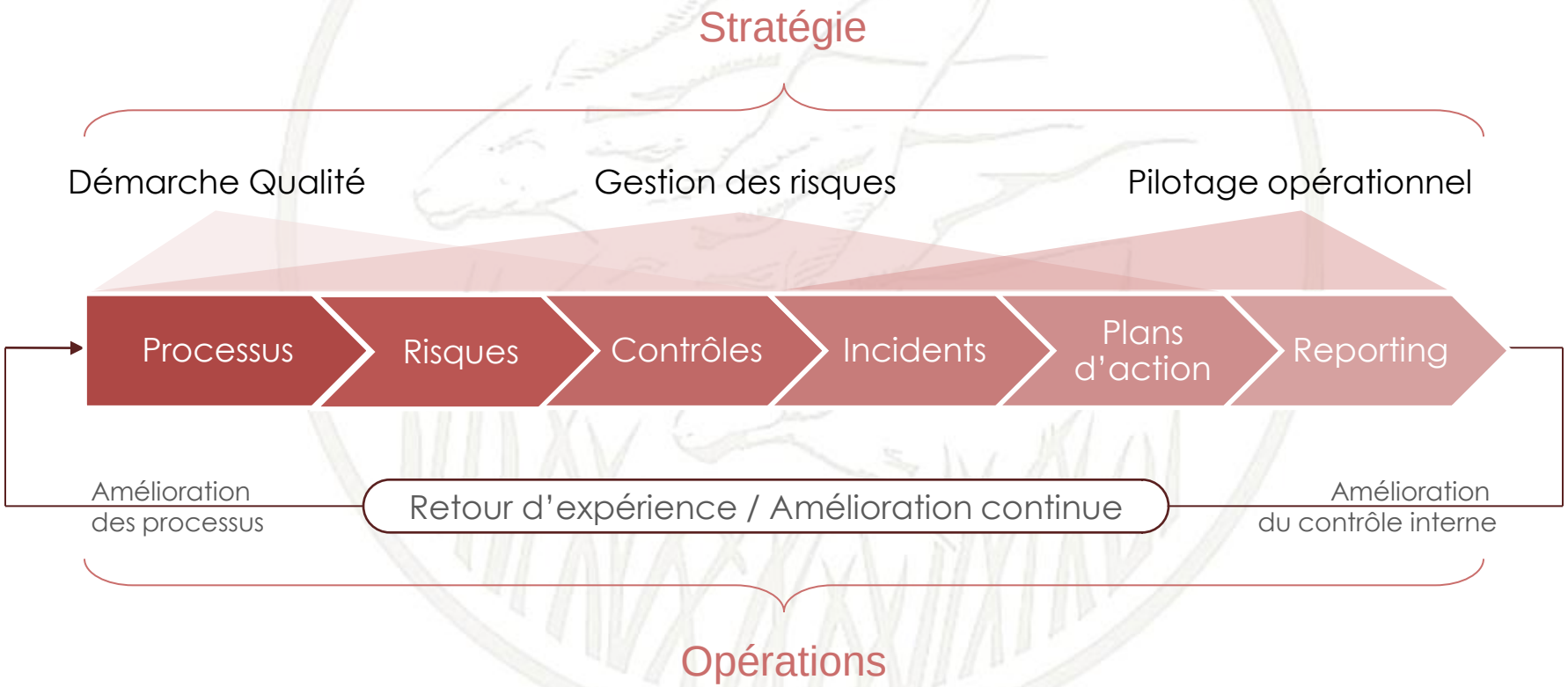
SOMMAIRE

Vision d'ensemble d'un dispositif de gestion des risques opérationnels

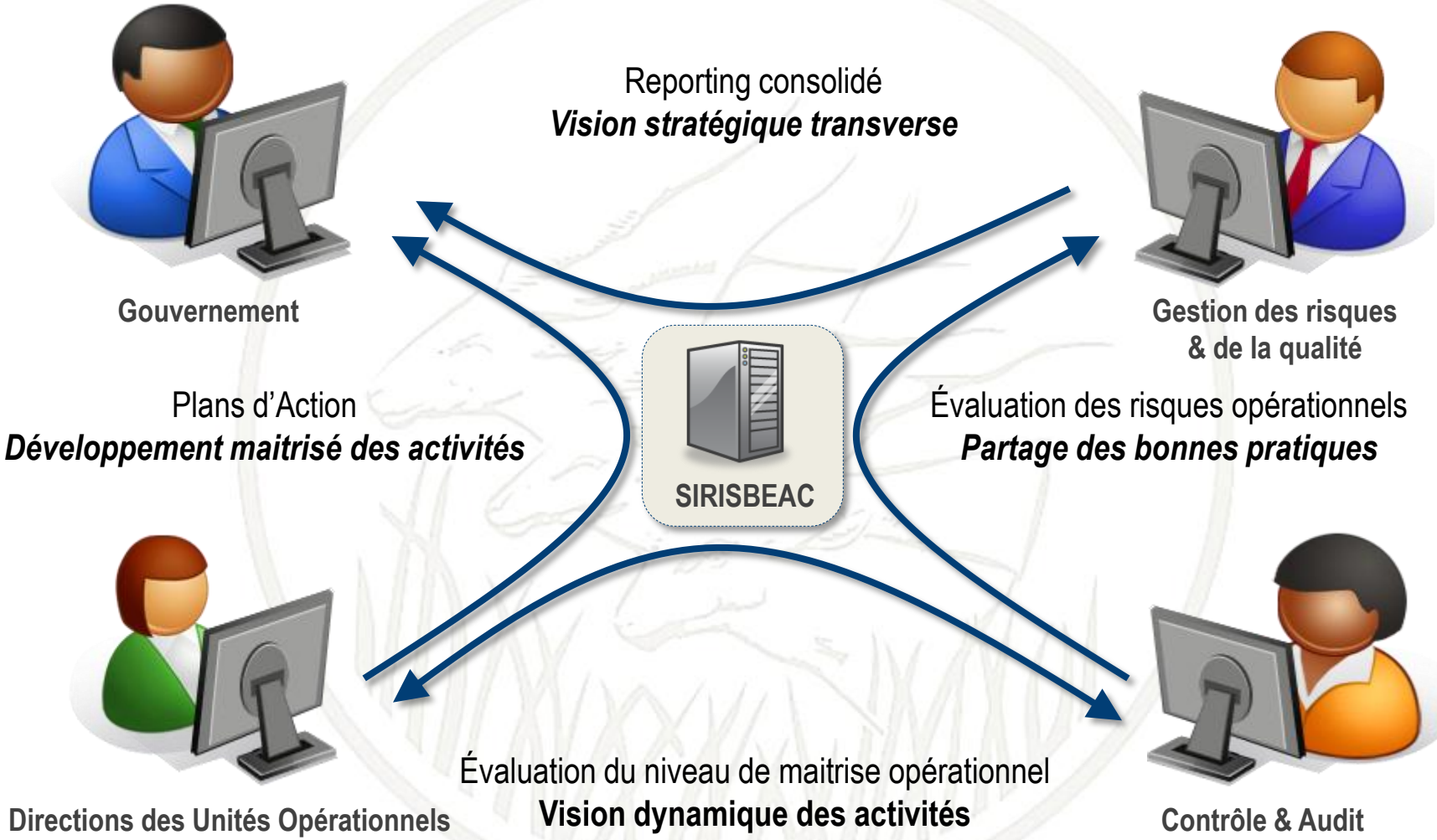


SIRISBEAC, une amorce pour une gestion maîtrisée des activités

SIRISBEAC permettra de **collecter / coordonner / consolider / formaliser** les données pertinentes pour la maitrise des activités de chaque métier



Un outil pour fluidifier les échanges



Fréquence du Reporting

Le reporting se fait selon une périodicité variable (mensuelle, trimestrielle, semestrielle, annuelle) en fonction des destinataires, des réglementations et du pilotage des risques.

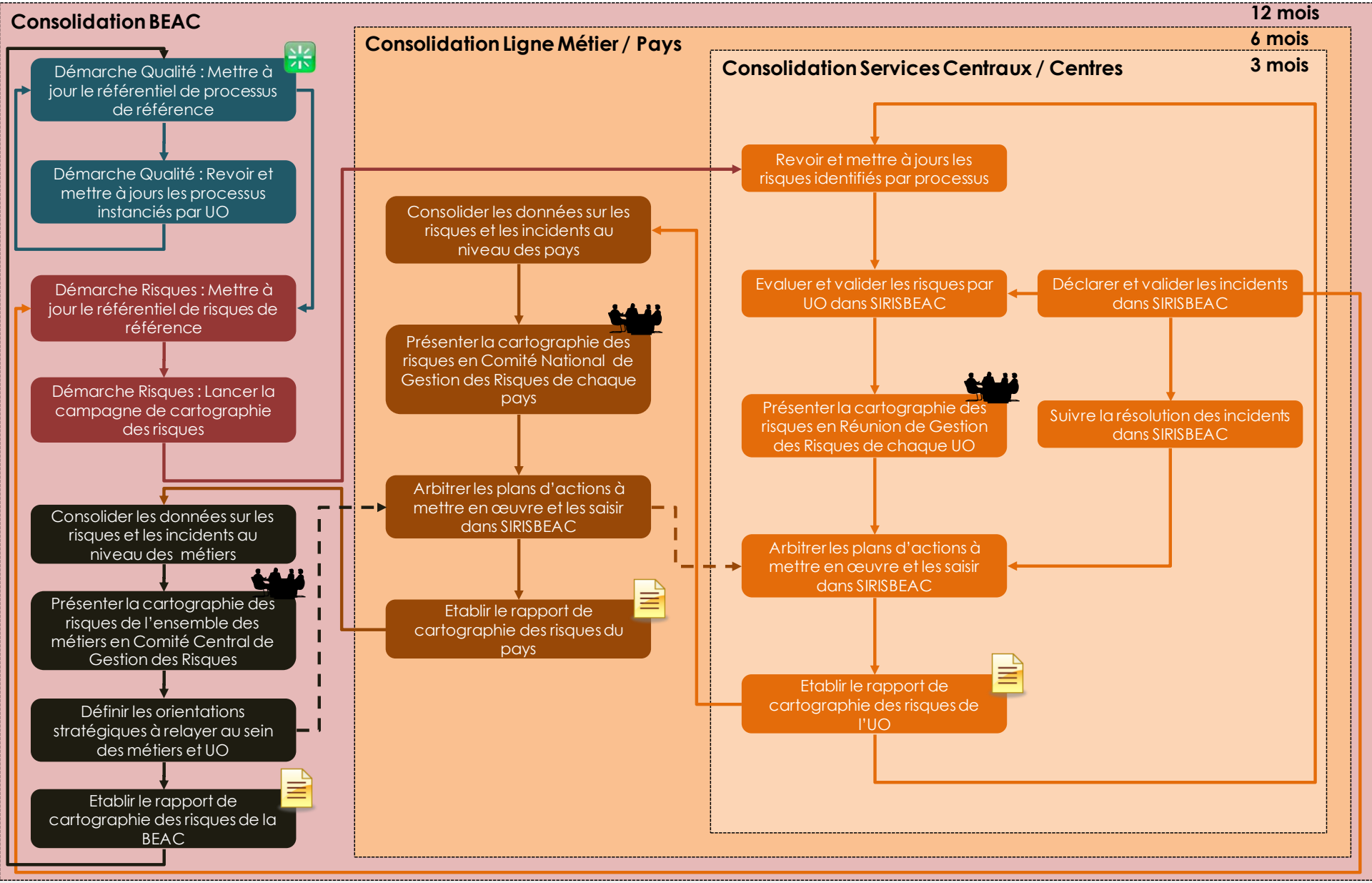
Format du Reporting

Le format du reporting est le même pour les Centres (Directions Nationales, Agences, Bureaux) et les Services Centraux à fin d'en faciliter la lecture et de simplifier les comparaisons afin d'assurer les synergies.

Le format du reporting dépendra de sa fonction et de sa granularité. Ainsi la méthodologie DEMARIS et l'outil SIRISBEAC définissent deux types de reporting :

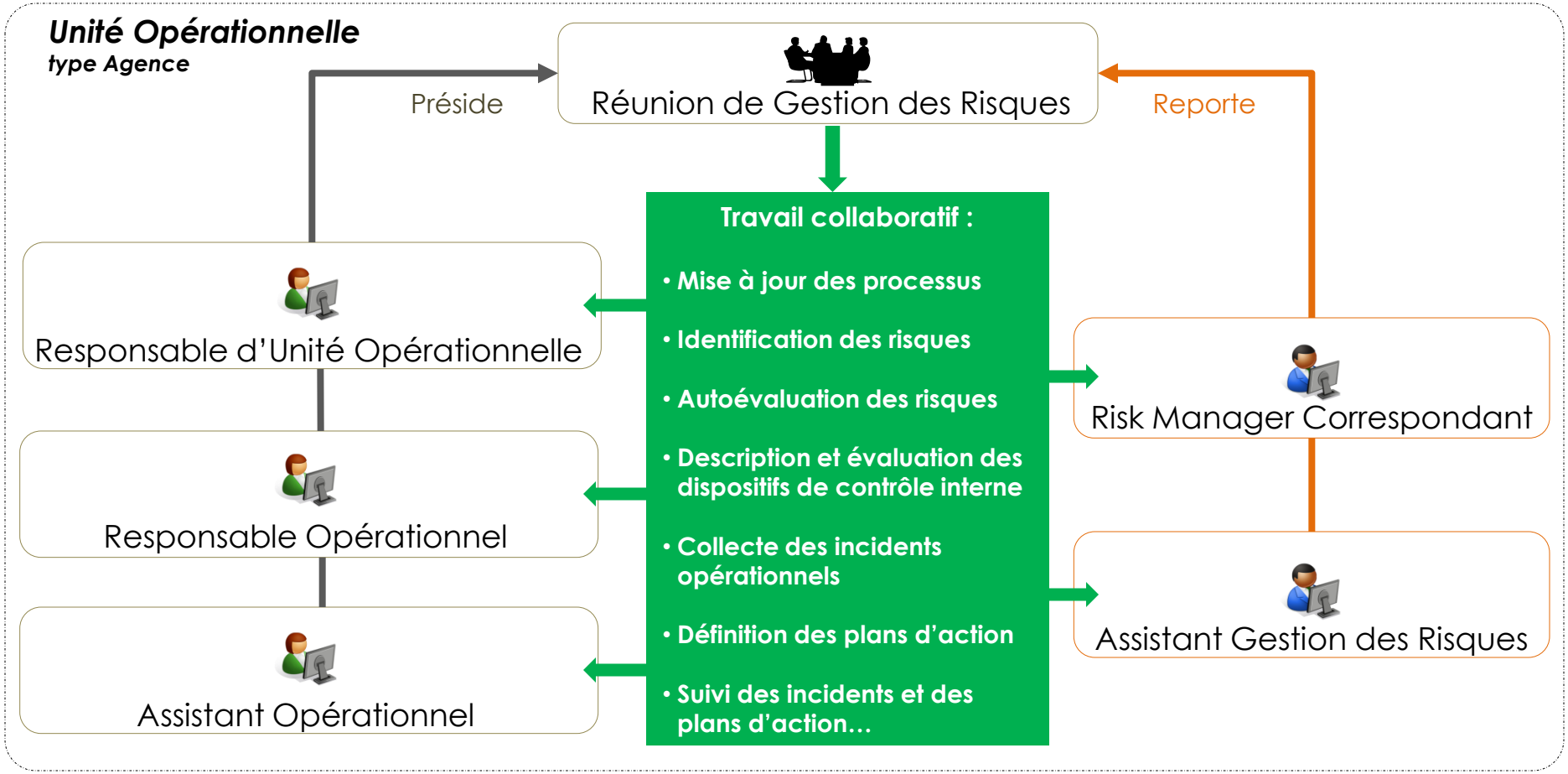
- le reporting standardisé
- le reporting paramétré

Exemple de modélisation d'une démarche intégrée

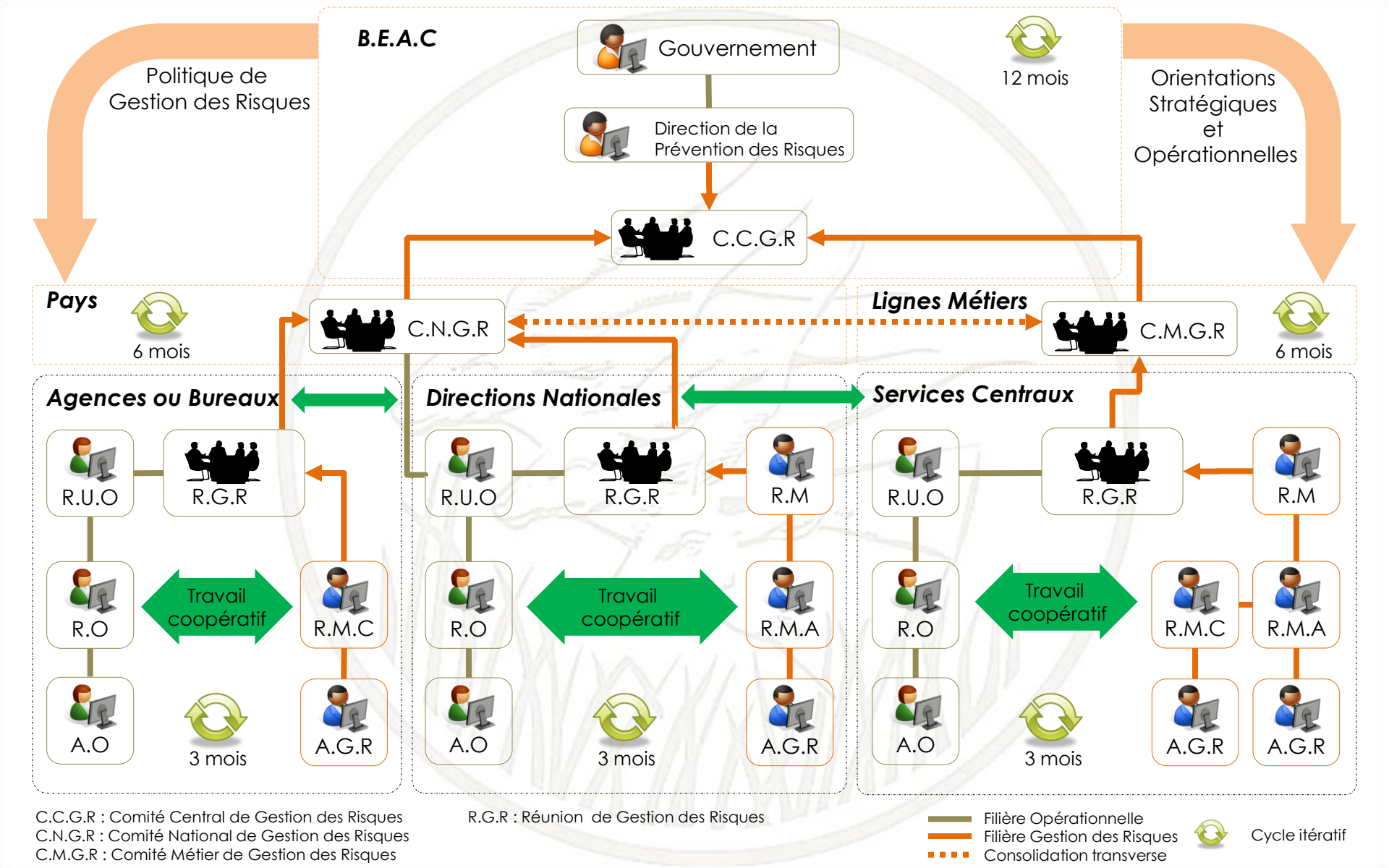


Un mode d'évaluation coopératif

L'organisation de la gestion des risques s'appuie sur un **dispositif collaboratif au sein des unités opérationnelles** entre les acteurs opérationnels et des relais d'expertise identifiés et formés à la méthodologie DEMARIS.



Exemple de modélisation d'une organisation adaptée



Méthodologie DEMARIS

<< FIN DU DOCUMENT >>