La révision du cadre de gestion du risque opérationnel au service de l'efficacité de la gestion du risque opérationnel dans le système bancaire[1].

Table des matières

1. Gestion du risque opérationnel

1.1. Définition

- Le risque opérationnel se défini dans le cadre de la gestion des fonds propres comme le risque de perte résultant de processus internes inadéquats ou défaillants ou d'événements extérieurs.
    - Cette définition **inclut le risque juridique mais exclut le risque stratégique et le risque de réputation**.
- Le **risque opérationnel est inhérent à tous les produits, activités, processus et systèmes** bancaires. La gestion efficace du risque opérationnel est un élément fondamental du dispositif de gestion des risques d'une banque. **Une gestion saine du risque opérationnel est le reflet de l'efficacité du conseil et de la direction générale** dans l'administration de leur dispositif de gestion des risques liés au portefeuille de produits, d'activités, de processus et de systèmes de la banque.

[1] Revisions to the Principles for the Sound Management of Operational Risk - March 2021-

- Si **la gestion du risque opérationnel et la résilience opérationnelle** visent des objectifs différents, ces deux notions sont néanmoins étroitement liées.
    - **Un système de gestion du risque opérationnel efficace et un niveau solide de résilience opérationnelle fonctionnent de concert** pour réduire la fréquence et l'impact des événements de risque opérationnel.
- **Une gestion saine du risque** permet à la banque de mieux appréhender et gérer son profil de risque.
- La gestion des risques comprend :
    - L'identification des risques auxquels la banque est exposée ;
    - La mesure et l'évaluation de l'exposition à ces risques (si possible) ;
    - Le suivi de l'exposition aux risques et l'élaboration d'un plan d'action ;
    - Le suivi permanent des expositions et des besoins en capital correspondants ;
    - La mise en œuvre de dispositifs pour contrôler ou atténuer les expositions ;
    - Faire un rapport à la direction générale et au conseil sur les expositions aux risques et les besoins en capital de la banque.
- Les contrôles internes sont généralement intégrés dans les activités quotidiennes d'une banque et sont conçus pour garantir, dans la mesure du possible, que :
    - Les activités de la banque sont efficientes et efficaces ;
    - L'information est fiable, opportune et qu'elle peut être utilisée à bon escient ;
    - La banque se conforme aux lois et règlements applicables.

1.2. Une gouvernance interne saine, fondement d'un CGRO efficace.

- La gouvernance de la gestion du risque opérationnel présente des similitudes mais aussi des différences par rapport à la gestion du risque de crédit ou du risque de marché.
- Pour assurer la résilience opérationnelle, une banque doit partir prendre en compte de possibles perturbations dans la définition de son appétence au risque et les limites fixées dans le cadre de la tolérance au risque.
- La résilience opérationnelle suppose de définir le niveau de tolérance par rapport aux incidents opérationnels.
- La gouvernance du risque opérationnel des banques doit être pleinement intégrée à la gouvernance globale de la gestion des risques.

1.3. Le rôle des 3 lignes de défense (maîtrise)

- Les banques s'appuient généralement sur **trois lignes de défense** :
    - La 1ère ligne :
        - Gestion des unités d'affaires (fonction de production, unité opérationnelle) ;
    - La 2ème ligne
        - Une fonction indépendante de gestion du risque opérationnel de l'entreprise (CORF) (2ème niveau de contrôle au sens de l'arrêté du 25 février 2021 en France);
    - La 3ème ligne
        - Une assurance indépendante (audit-inspection, 3ème niveau de contrôle au sens de l'arrêté ci-dessus).
- Ces 3 lignes sont adaptées à la nature, la taille et la complexité de la banque, ainsi que le profil de risque de ses activités.

- **Les conditions de réussite de ces 3 lignes**[2] supposent que la banque respecte les principes suivants :
    - Des ressources adéquates en termes de budget, d'outils et de personnel ;
    - Des rôles et des responsabilités clairement définis ;
    - Du personnel compétent et formé de manière continue et adéquate ;
        - La diffusion d'une culture saine de gestion des risques dans l'ensemble de l'organisation ;
- Des interactions et des échanges d'information entre les lignes de défense.
- Cas des unités opérationnelles où co-existent des fonctions de première et de deuxième ligne de défense
    - Bien documenter et distinguer les responsabilités de ces fonctions au sein de la première et de la deuxième ligne de défense, en soulignant l'indépendance de ces fonctions.
- **Le périmètre de responsabilité**
    - La direction de l'unité opérationnelle est responsable de l'identification et de la gestion des risques inhérents aux produits, activités, processus, etc. dont elle est responsable. Les banques doivent disposer d'une **politique qui définit clairement les rôles et les responsabilités des unités opérationnelles concernées**.
- **Les éléments-clés d'une première ligne de défense efficace** dans la promotion d'une culture saine de gestion du risque opérationnel :
    - L'identification et l'évaluation de l'importance des risques opérationnels inhérents aux unités d'affaires respectives, par le biais de la gestion du risque opérationnel et des outils associés.
    - L'établissement de contrôles appropriés pour atténuer les risques opérationnels inhérents, et évaluer la conception et l'efficacité de ces contrôles en utilisant les outils de gestion des risques opérationnels.
    - Le signalement rapide de tout défaut dans l'adéquation des ressources, des outils et/ou de la formation pour assurer l'identification et l'évaluation des risques opérationnels ;
    - La surveillance des profils de risque opérationnel des unités d'affaires et la nécessité de rendre compte, et d'assurer la conformité des profils à l'appétence pour le risque opérationnel qui a été préalablement défini et les seuils de tolérance.
    - Le signalement des risques opérationnels résiduels après prise en compte des contrôles ainsi que les pertes opérationnelles, les déficiences des contrôles, les insuffisances des processus et le non-respect des seuils de tolérances en matière de risque opérationnel.
- Une deuxième ligne de défense composée notamment d'une fonction de gestion du risque opérationnel indépendante
    - Un CGRO fonctionnellement indépendant constitue généralement la deuxième ligne de défense.
    - Les responsabilités d'une deuxième ligne de défense efficace devraient inclure :
        - L'élaboration d'une opinion indépendante concernant
            - Les risques opérationnels identifiés au sein des unités d'affaires
            - La conception et l'efficacité des contrôles clés
            - Et la tolérance au risque ;

[2] Le document du Comité de Bâle profite de cette mise à jour pour préciser le rôle de ces 3 lignes et l'adaptation selon les enjeux de l'établissement (proportionnalité).

        - La possibilité de remise en question de la pertinence et de la cohérence de la mise en œuvre par l'unité d'affaires des outils de gestion du risque opérationnel, des activités de mesure et des systèmes de reporting, et en fournissant des éléments factuels justifiant cette remise en cause ou évolution ;
        - L'élaboration et la mise à jour des politiques, des normes et des directives en matière de gestion et de mesure du risque opérationnel ;
        - L'analyse et le suivi du profil de risque opérationnel ;
        - La conception et l'animation de la formation sur le risque opérationnel ;
        - Le développement d'une culture du risque.
    - **Le degré d'indépendance de la fonction gestion des risques opérationnels (CGRO) peut varier selon les banques**. Dans les petites banques, l'indépendance repose généralement sur la séparation des tâches et l'examen indépendant des processus et des fonctions. Dans les grandes banques, la CGRO doit faire partie d'une structure hiérarchique indépendante des unités d'affaires génératrices de risques et être responsable de la conception, de la maintenance et du développement continu du système de contrôle interne.
    - Le CGRO s'appuie généralement sur d'autres fonctions qui contribuent à la maîtrise des risques tels les services de conformité, juridique, financier et informatique (IT) pour l'aider à évaluer le niveau de risque de la banque.
    - Les banques doivent avoir une politique qui définit clairement les rôles et responsabilités de la CGRO, en fonction de la taille et de la complexité de l'organisation.
- **La troisième ligne de défense** fournit une assurance indépendante au conseil quant au caractère approprié du cadre de gestion des risques opérationnels de la banque.
    - Les collaborateurs de la 3ème ligne ne peuvent être impliqués dans l'élaboration, la mise en œuvre et le fonctionnement des processus de gestion du risque opérationnel de la banque des 1ères et 2ème lignes.
        - Les travaux du ressort de la 3ème ligne peuvent être réalisés par les auditeurs internes, externes ou d'autres tiers indépendants dûment qualifiés.
    - L'étendue et la fréquence des revues doivent être suffisantes pour couvrir toutes les activités et entités juridiques d'une banque.
    - Les éléments-clés d'une revue indépendante efficace :
        - Examen de la conception et de la mise en œuvre des systèmes de gestion du risque opérationnel et des processus de gouvernance associés à la 1ère et 2ème ligne de défense (y compris l'indépendance de cette dernière)
        - Examen des processus de validation pour s'assurer qu'ils sont indépendants et mis en œuvre d'une manière cohérente avec les politiques établies de la banque
        - Assurance que les systèmes de quantification utilisés par la banque sont suffisamment robustes c'est-à-dire :
            - Qu'ils fournissent l'assurance raisonnable quant à l'intégrité des entrées, des hypothèses, des processus et de la méthodologie qu'ils fournissent
            - Et qu'ils aboutissent à des évaluations du risque opérationnel qui reflètent de manière crédible le profil de risque opérationnel de la banque ;

        - L'assurance que la direction des unités d'affaires répond rapidement, avec précision et de manière adéquate aux questions soulevées, et rende régulièrement compte au conseil ou à des comités dédiés des questions en suspens et leur résolution ;
        - Emission d'avis sur la pertinence et l'adéquation globales du Cadre de gestion des risques de l'entreprise et des processus de gouvernance associés dans l'ensemble de la banque.
    - **Outre la conformité du dispositif, la 3ème ligne doit mener une revue indépendante afin d'évaluer si le CGRO répond aux besoins et aux attentes de l'organisation** (respect de l'appétit et de la tolérance de l'entreprise pour le risque, adaptation du cadre aux besoins de l'organisation, etc.) tout en étant conforme aux dispositions statutaires et législatives, aux accords contractuels, aux règles internes et à l'éthique.
- **Responsabilité de la Direction Générale**
    - La Direction Générale doit s'assurer que les politiques, les processus et les systèmes du CGRO sont suffisamment robustes pour gérer et garantir que les pertes opérationnelles sont traitées de manière adéquate et en temps utile. Cela est d'autant plus important que l'environnement est en constante évolution.

L'amélioration de la gestion du risque opérationnel dépend fortement de la volonté de la haute direction d'être proactive et d'agir rapidement.

2. Principes pour une gestion saine du risque opérationnel

Le Comité définit 12 principes pour une saine gestion du risque opérationnel.

2.1. Culture de gestion du risque

Principe 1 : Le conseil doit être à l'initiative d'une solide culture de gestion du risque, mise en œuvre par la direction générale. Le conseil et la direction générale doivent instaurer une culture d'entreprise guidée par une forte gestion du risque, fixer des normes et des incitations à un comportement professionnel et responsable, et veiller à ce que le personnel reçoive une formation appropriée en matière de gestion des risques et d'éthique.

- Les banques dotées d'une forte culture de gestion des risques et de pratiques commerciales éthiques sont moins susceptibles de subir des événements dommageables liés au risque opérationnel et sont moins susceptibles d'être touchées par la crise et mieux placées pour faire face efficacement aux événements qui se produisent.
- Les actions du conseil et de la direction générale, ainsi que les politiques, les processus et les systèmes de gestion des risques de la banque, fournissent le cadre nécessaire à la gestion du risque opérationnel. Ces éléments sont à la base d'une bonne culture de gestion des risques.
- **Le conseil devrait établir un code de conduite ou une politique d'éthique** pour traiter le risque lié à des comportements inappropriés. Ce code ou cette politique doit s'appliquer à la fois au personnel et aux membres du conseil et s'appuyer sur de fortes exigences éthiques. Il s'agit également d'identifier les pratiques commerciales acceptables ainsi que les conflits d'intérêts ou la fourniture inappropriée de services financiers (que ce soit intentionnellement ou par négligence).
    - Le code ou la politique doit être régulièrement revu et approuvé par le conseil et attesté par les employés. Sa mise en œuvre doit être supervisée par un comité d'éthique ou un autre comité du conseil et doit être accessible au public (par

exemple sur le site web de la banque). Un code de conduite spécifique peut être établi pour des postes spécifiques au sein de la banque (par exemple, front-office en salle des marchés, preneurs de risque).

- **Le management doit fixer des attentes et des responsabilités claires** pour s'assurer que le personnel de la banque appréhende correctement son rôle et ses responsabilités en matière de gestion des risques, et dispose de l'autorité nécessaire pour exercer ces responsabilités.
- **Les politiques de rémunération devraient être alignées sur la déclaration d'appétence et de tolérance au risque de la banque**, ainsi que sur la sécurité et la solidité globales de la banque. L'équilibre doit être trouvé entre l'incitation et la prise de risque.
- L'encadrement supérieur doit veiller à ce **qu'un niveau approprié de formation au risque opérationnel** soit disponible à tous les niveaux dans l'ensemble de l'organisation, y compris au sein de la direction générale. Ainsi les responsables des unités opérationnelles, les responsables des contrôles internes et les cadres supérieurs devraient disposer de formations adaptées.
    - La formation dispensée doit refléter l'ancienneté, le rôle et les responsabilités des personnes auxquelles elle est destinée.
- **Le tone from the top est ré-affirmé** : le conseil et de la direction générale ainsi que l'encadrement doivent apporter un soutien fort à la gestion du risque opérationnel et à un comportement éthique convaincant, ce qui permet de renforcer le rôle des codes de conduite et d'éthique, les stratégies de rémunération et les programmes de formation.

Principe 2 : Les banques doivent élaborer, mettre en œuvre et maintenir un cadre de gestion du risque opérationnel totalement intégré à leur organisation.

Le dispositif de gestion du risque opérationnel adopté par la banque dépendra d'un ensemble de facteurs dont la nature des activités, la taille, la complexité des opérations et son profil de risque.

- **Le conseil et la direction de la banque doivent comprendre la nature et la complexité des risques inhérents au portefeuille de produits, de services**, d'activités et de systèmes de la banque, ce qui est un principe fondamental d'une saine gestion des risques.
    - Ceci est particulièrement important pour le risque opérationnel, étant donné que le risque opérationnel est inhérent à tous les produits commerciaux, activités, processus et systèmes de la banque.
- Les composantes du dispositif CGRO doivent être pleinement intégrées dans les processus globaux de gestion des risques de la banque par les responsables de première ligne, examinés et remis en question de manière adéquate par la deuxième ligne de défense, et examinés de manière indépendante par la troisième ligne de défense.
    - La CGRO doit être intégré à tous les niveaux de l'organisation, y compris le groupe et les unités d'affaires, ainsi que toutes les évolutions de produits, activités, processus et systèmes
    - En outre, **les résultats de l'évaluation du risque opérationnel de la banque doivent être intégrés dans le processus de développement de la stratégie** commerciale de la banque.
- Le dispositif de gestion du risque opérationnel doit être documenté de manière complète et appropriée dans des politiques approuvées par le conseil et **inclure des définitions du risque opérationnel et de la perte opérationnelle.** Les banques qui ne décrivent pas et ne classent pas de manière adéquate le risque opérationnel et l'exposition aux pertes peuvent réduire considérablement l'efficacité de leur CGRO.
- **La documentation liée à la CGRO** devrait clairement :

- **Identifier les structures de gouvernance utilisées pour gérer le risque opérationnel**, y compris les lignes hiérarchiques et les responsabilités, ainsi que les mandats et la composition des membres du comité de gouvernance du risque opérationnel.
- S'appuyer sur des politiques et procédures pertinentes de gestion du risque opérationnel ;
- **Documenter les outils d'identification et d'évaluation** des risques et des contrôles, ainsi que le rôle et les responsabilités des trois lignes de défense dans la gestion du risque opérationnel ;
- Décrire l'appétence et la tolérance au risque opérationnel de la banque ; les seuils, les indicateurs opérationnels ou les limites pour les risques inhérents et les risques liés à l'activité ; les stratégies et les instruments validés permettant d'atténuer le risque ;
- Décrire l'approche de la banque pour s'assurer que les contrôles sont conçus, mis en œuvre et fonctionnent de manière efficace ;
- Décrire les modalités d'établissement et de suivi des seuils ou limites d'exposition aux risques inhérents et résiduels ;
- Identifier les risques et les contrôles mis en œuvre par toutes les unités opérationnelles (par exemple dans le référentiel de contrôles) ;
- Mettre en place des systèmes de reporting des risques et de management de l'information (SMI) permettant la production de données précises et en temps voulu ;
- Prévoir une taxonomie commune des termes associés au risque opérationnel afin d'assurer la cohérence de l'identification des risques, de l'évaluation de l'exposition et des objectifs de gestion du risque au sein de toutes les unités opérationnelles en fonction des types d'événements, de leurs causes, de leur importance relative et de leur nature.

2.2 Rôle du Conseil

Principe 3 : Le conseil approuve et revoit périodiquement le cadre de gestion du risque opérationnel. Il s'assure que la direction générale met en œuvre les politiques, les processus et les systèmes du cadre de gestion du risque opérationnel de manière efficace à tous les niveaux de décision.

- Le conseil devrait :
  - **Etablir une culture de gestion du risque** et s'assurer que la banque dispose de processus adéquats pour comprendre la nature et la portée du **risque opérationnel inhérent aux stratégies et activités actuelles et prévues de la banque ;**
  - **Veiller à** ce que les processus de gestion du risque opérationnel fassent l'objet **d'une surveillance exhaustive et dynamique** et qu'ils soient pleinement intégrés dans la stratégie et l'ensemble des activités de la banque.
  - **Fournir à l'encadrement supérieurs des directives claires concernant les principes qui sous-tendent le cadre de gestion du risque opérationnel (CGRO)**, et approuver les politiques correspondantes élaborées par la direction générale pour s'aligner sur ces principes ;
  - **Examiner et évaluer régulièrement l'efficacité du Cadre** de gestion du risque opérationnel, et l'approuver, afin de s'assurer que la banque a identifié et gère le risque opérationnel découlant de l'évolution des facteurs externes tels les facteurs environnementaux, ainsi que le risque opérationnel lié à l'évolution de nouveaux

produits, activités, processus ou systèmes, y compris les changements de profils de risque et de priorités (par exemple, l'évolution du PNB de certains métiers) ;
    - **S'assurer que le dispositif CGRO** de la banque fait **l'objet d'un examen indépendant effectif** par une troisième ligne de défense (audit ou autres tiers indépendants de sources externes ayant reçu une formation appropriée) ; et
    - S'assurer que, au fur et à mesure de l'évolution des meilleures pratiques, la direction tire parti de ces avancées.
- Des contrôles internes solides sont une composante essentielle de la gestion du risque opérationnel. **Le conseil doit établir des lignes claires de responsabilité et d'obligation de rendre compte** pour la mise en place d'un environnement de contrôle solide. Les contrôles doivent être régulièrement révisés, surveillés et testés afin de garantir leur efficacité.
    - L'environnement de contrôle doit assurer une indépendance/séparation des tâches appropriée entre les fonctions de gestion du risque opérationnel, les unités opérationnelles et les fonctions support (RH, Qualité, Finance, notamment).

Principe 4 : Le conseil approuve et révise périodiquement une déclaration d'appétit pour le risque et de tolérance au risque opérationnel[3], qui précise la nature, les types et les niveaux de risque opérationnel que la banque est prête à assumer.

- **La déclaration d'appétit pour le risque et de tolérance au risque opérationnel est élaborée sous l'autorité du conseil** et liée aux plans stratégiques et financiers à court et à long terme de la banque. Cette déclaration doit être en phase avec la capacité en risque de la banque, en prenant en compte notamment les intérêts des clients et des actionnaires de la banque ainsi que des exigences réglementaires.
- Caractéristiques d'une déclaration efficace d'appétit pour le risque et de tolérance au risque efficace :
    - Être facile à communiquer et donc à comprendre pour toutes les parties prenantes ;
    - inclure les informations de base et les hypothèses clés qui ont servi de base aux plans d'activité (Business Model) de la banque au moment où elle a été approuvée ;
    - inclure des déclarations qui expriment clairement les raisons d'assumer ou d'éviter certains types de risques, et établir des limites ou des indicateurs (quantitatifs ou non) permettant de surveiller le suivi de ces risques ;
    - s'assurer que la stratégie et les limites de risque des unités opérationnelles et des entités juridiques, selon le cas, sont conformes à la déclaration d'appétence au risque de la banque et adaptée aux enjeux de la banque;
    - être prospectifs et, le cas échéant, faire l'objet de scénarios et de simulations de crise pour garantir que la banque comprend quels événements pourraient la pousser à dépasser sa déclaration d'appétit pour le risque et de tolérance.
- Le conseil devrait **approuver et revoir régulièrement la pertinence des limites** et de la déclaration globale d'appétence et de tolérance au risque opérationnel.
- Cet examen doit prendre en compte les changements actuels et prévus dans l'environnement externe (y compris le contexte réglementaire dans toutes les juridictions où l'institution fournit des services), les changements en cours et les changements prévus dans l'environnement externe ; les augmentations significatives en cours ou à venir de l'activité ou du volume d'affaires ainsi que la qualité de l'environnement de contrôle ; l'efficacité des

[3] Document de type Risk Appetite Framework (RAF) encadré par le Risk Appetite Statement (RAS). En matière de risque opérationnel, il est fréquent de trouver des indicateurs du type 'coût du risque opérationnel', ' taux de fraude', 'taux de formation', 'taux de réclamation' etc. selon les types d'activité et les enjeux de la banque.

stratégies de gestion ou d'atténuation des risques ; l'expérience en matière de pertes (à partir notamment de la collecte des pertes et des incidents) ; et la fréquence, le volume ou la nature des dépassements de limites.

- **Le conseil doit surveiller l'adhésion de la direction à l'appétence pour le risque** et à la déclaration de tolérance, et prévoir la détection et la correction en temps utile des dépassements significatifs.

2.3. Rôle des instances dirigeantes

Principe 5 : La direction générale élabore, pour approbation par le conseil n, une structure de gouvernance claire, efficace et solide, avec des lignes de responsabilité bien définies, transparentes et cohérentes.

- Les instances dirigeantes sont responsables de la mise en œuvre et du suivi efficace sur tout le périmètre de l'établissement des politiques, processus et des systèmes de gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants de la banque, conformément à la déclaration d'appétence et de tolérance au risque de la banque.
- Les instances dirigeantes sont **responsables de la mise en place et du suivi d'un dispositif d'évaluation et d'identification des dysfonctionnements significatifs** et ont mis en œuvre des **processus efficaces de résolution des problèmes**.
    - Ceux-ci doivent comprendre des systèmes permettant de signaler, de suivre et, si nécessaire, de transmettre les problèmes à un échelon supérieur afin de s'assurer qu'ils sont correctement gérés, si nécessaire, de faire remonter les problèmes afin de les résoudre.
    - Les banques devraient être en mesure de **démontrer que l'approche des trois lignes de défense** fonctionne de manière satisfaisante et d'expliquer comment le conseil, le comité d'audit (et des risques) indépendant du conseil et la direction générale s'assure de cette efficacité.
- La direction générale doit traduire le Cadre de gestion des risques de l'entreprise (CGR) approuvé par le conseil en politiques et procédures spécifiques pouvant être mises en œuvre et vérifiées au sein des différentes unités d'affaires. La direction générale doit définir des niveaux de responsabilités (autorité, limites, délégation) précises afin d'encourager et de maintenir l'obligation de rendre des comptes et de garantir que les mesures nécessaires sont prises.
    - Elle s'assure également que **les ressources nécessaires sont disponibles** pour gérer le risque opérationnel conformément à l'appétit pour le risque de la banque.
    - En outre, la direction générale doit s'assurer que le processus de surveillance par le management est adapté aux risques inhérents des lignes métiers/ activité sous responsabilité managériale.
- **Interactions entre les métiers** : La direction générale doit s'assurer que le personnel responsable de la gestion du risque opérationnel coordonne et communique efficacement avec le personnel chargé de la gestion du risque de crédit, du risque de marché et des autres risques, ainsi qu'avec les personnes chargées de gérer le transfert (partage) du risque avec notamment les compagnies d'assurance ou dans le cadre d'une externalisation.
    - Le cas échéant, le cadre de gestion des risques pourrait souffrir de dysfonctionnements importants et de source d'inefficacité.
- **Les responsables du CGRO devraient avoir une autorité suffisante au sein de la banque** pour s'acquitter efficacement de leurs fonctions, ce qui se traduit généralement par un

niveau de responsabilité correspondant à d'autres fonctions de gestion des risques, telles que le risque de crédit, de marché et de liquidité[4].

- La direction générale doit veiller à ce que les activités de la banque soient menées par **un personnel possédant l'expérience, les compétences techniques** et l'accès aux ressources nécessaires et l'accès aux ressources nécessaires. Le personnel chargé de surveiller et de faire respecter la politique de risque de l'établissement doit avoir une autorité indépendante des unités qu'il supervise.
- **La structure de gouvernance d'une banque devrait être adaptée à la nature, à la taille, à la complexité et au profil de risque** de ses activités.
- Lors de la conception de la structure de gouvernance du risque opérationnel, une banque devrait prendre en compte les éléments suivants :
    - **Structure des comités** - Une pratique saine dans le secteur consiste à mettre en place dans les grands groupes une fonction centrale et des unités opérationnelles distinctes, ainsi qu'un comité des risques[5] créé par le conseil au niveau de l'entreprise pour superviser tous les risques auquel rend compte un comité de gestion du risque opérationnel.
    - En fonction de la nature, de la taille et de la complexité de la banque, le comité des risques au niveau de la banque peut être alimenté par les comités des risques opérationnels par pays, par secteur d'activité ou par domaine fonctionnel**.**
    - Les organisations plus petites et moins complexes peuvent utiliser une structure organisationnelle simplifiée où le risque opérationnel peut être directement supervisé au sein du comité de gestion des risques du conseil.
    - Composition du comité[6] risque opérationnel (ou le comité de risque dans les petites banques) : des membres ayant une expertise variée, telle une expertise dans les activités commerciales, les activités financières, les questions juridiques, technologiques et réglementaires, et une gestion indépendante des risques.
    - Fonctionnement du comité
        - Les réunions du comité doivent être organisées à une fréquence appropriée, selon une durée et avec des ressources appropriées pour permettre des échanges constructifs.
        - Les comptes rendus des fonctionnements du comité doivent être adéquats afin de permettre l'examen et l'évaluation de son efficacité.

3. Environnement de gestion des risques

3.1. Identification et évaluation

[4] L'objectif étant de ne pas considérer la gestion du risque opérationnel comme un sous-risque par rapport aux risques financiers.

[5] Comité des risques Groupe (qui rapporte au Comité d'audit et des risques) auquel rapporte un comité spécifique risque opérationnel (qui traite généralement au sein du même comité les enjeux de contrôles opérationnels-contrôle permanent) ; Dans les grands groupes, la conformité fait l'objet d'un comité spécifique eu égard à l'importance des sujets)

[6] 2015 Corporate governance principles for banks for additional requirements on the Committee composition

Principe 6 : La direction générale doit veiller à l'identification et à l'évaluation complètes *du risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants, afin de s'assurer que les liens entre prise de risque et incitations sont bien compris.*

- L'identification et l'évaluation des risques sont des caractéristiques fondamentales d'un système efficace de gestion du risque opérationnel et contribuent directement aux capacités de résilience opérationnelle.
    - **L'identification efficace des risques tient compte à la fois des facteurs internes et des facteurs externes**. Une bonne évaluation des risques permet à la banque de mieux comprendre son profil de risque et d'allouer les ressources et les stratégies de gestion des risques de la manière la plus efficace.
- **Voici des exemples d'outils utilisés pour identifier et évaluer le risque opérationnel :**
    - **Gestion des événements de risques (dont les pertes et incidents)**
        - Lorsqu'une banque est confrontée à un événement de risque opérationnel, le processus d'identification, d'analyse, de gestion et de déclaration de l'événement suit un ensemble prédéterminé de processus. Une bonne approche de la gestion des événements comprend généralement l'analyse des événements afin d'identifier de nouveaux risques opérationnels, de comprendre les causes sous-jacentes et les dysfonctionnements de contrôle, et de formuler des recommandations appropriées pour éviter que des événements similaires ne se reproduisent.
            - Ces informations constituent un apport à l'auto-évaluation et, en particulier, à l'évaluation de l'efficacité du contrôle.
    - **Données sur les événements liés au risque opérationnel**
        - Les banques conservent souvent un ensemble complet de données sur les événements liés au risque opérationnel, qui rassemble tous les événements importants vécus par la banque et sert de base à l'évaluation du risque opérationnel.
        - L'ensemble de données sur les événements comprend généralement des données sur les pertes internes, les incidents évités de justesse (*near miss*), et, lorsque cela est possible, des données externes sur les pertes opérationnelles (car les données externes renseignent sur les risques communs à l'ensemble du secteur).
        - Les données sur les événements sont généralement classées selon une taxonomie définie dans les politiques CGRO et appliquée de manière cohérente dans la banque.
        - Les données sur les événements comprennent généralement **la date de l'événement** (date de survenance, date de découverte et date de comptabilisation) et, dans le cas des événements de perte, **l'impact financier**. Dans le cas des pertes.
        - Lorsque d'autres informations sur les causes racines des événements sont disponibles, elles peuvent également être incluses dans l'ensemble de données sur le risque opérationnel. Lorsque cela est possible, les banques sont **encouragées à chercher à recueillir des données externes sur les événements de risque opérationnel et à les utiliser dans leur analyse interne**. En effet, elles sont souvent informatives sur les risques communs à l'ensemble du secteur.
    - **Auto-évaluations**

- **L**es banques procèdent souvent à des auto-évaluations de leurs risques et contrôles opérationnels à différents niveaux.
- Les évaluations portent généralement sur le risque inhérent (le risque avant que les contrôles ne soient pris en compte, risque brut), l'efficacité des contrôles et l'efficacité de la gestion des risques, l'efficacité de l'environnement de contrôle et le risque résiduel (le risque avant la prise en compte des contrôles – risque net).
- **L'élément qualitatif** reflète la prise en compte à la fois de la probabilité et de la conséquence de l'événement de risque dans la détermination par la banque de la cotation du risque inhérent et résiduel.
- **Les évaluations peuvent utiliser la cartographie des processus d'entreprise** pour identifier les étapes clés des processus d'entreprise, des activités et des fonctions organisationnelles, ainsi que les liens entre les processus d'entreprise et les fonctions organisationnelles ainsi que les risques associés et les domaines de faiblesse du contrôle.
- **Les évaluations contiennent des informations suffisamment détaillées sur l'environnement de l'entreprise**, les risques opérationnels, les causes sous-jacentes, les contrôles et l'évaluation de l'efficacité du contrôle pour permettre à un auditeur-contrôleur indépendant de déterminer comment la banque a mesuré ses risques et justifier le niveau de risque (et donc le profil).
- **Un référentiel des risques peut être tenu** pour rassembler ces informations afin d'obtenir une vision significative de l'efficacité globale des contrôles et faciliter la surveillance par la direction générale, les comités des risques et le conseil.

- **Cadre de surveillance et de maîtrise des risques**
  - L'intégration d'un cadre approprié de surveillance et de maîtrise des risques facilite une approche structurée de l'évaluation, de l'examen, de la surveillance continue et des tests des contrôles clés.
  - L'analyse des contrôles permet de s'assurer que ceux-ci sont conçus pour les risques identifiés et fonctionnent efficacement. L'analyse doit également tenir compte des éléments suivants :
  - Couverture suffisante des risques par les contrôles, y compris les stratégies adéquates de prévention, de détection et de réaction. Le suivi et les tests des contrôles doivent être adaptés aux différents risques opérationnels et aux contrôles clés dans les différents secteurs d'activité.
- **Mesure du risque**
  - En utilisant les données sur les événements liés au risque opérationnel et les évaluations des risques et des contrôles[7], les banques développent souvent des mesures pour évaluer et surveiller leurs risques opérationnels.
  - Ces mesures peuvent être de simples, comme le nombre d'événements, ou résulter de modèles d'exposition plus sophistiqués, le cas échéant.
  - Les mesures fournissent des informations d'alerte précoce pour surveiller la performance continue de l'entreprise et de l'environnement de contrôle, et

[7] La qualité des contrôles se mesure généralement selon une grille de cotation qui intègre différentes composantes (qualité des contrôles de la 1ère ligne, qualité des procédures, qualité de la formation, taux de réalisation des plans d'actions etc.).

rendre compte du profil de risque opérationnel. **Des mesures efficaces établissent un lien clair avec les risques opérationnels et les contrôles associés**.

- Le suivi des indicateurs et des facteurs de risque tant internes qu'externes au regard de limites définis fournit des informations précieuses pour améliorer la gestion des risques et le reporting.

- **Analyse de scénarios**
  - L'analyse de scénarios est une méthode permettant d'identifier, d'analyser et de mesurer une série de scénarios, y compris des **événements à faible probabilité (fréquence) et à gravité (impact- sévérité) élevée**, dont certains pourraient entraîner de graves pertes liées au risque opérationnel.
  - L'analyse de scénarios implique généralement **des réunions en atelier d'experts** incluant également des membres des instances dirigeantes et du management supérieur ainsi que des représentants des domaines fonctionnels tels que la conformité, les ressources humaines et la gestion des risques informatiques, afin de développer et analyser les facteurs et les conséquences d'événements potentiels. Les données utilisées pour l'analyse des scénarios comprendront généralement des **données pertinentes sur les pertes internes et externes, des informations provenant d'auto-évaluations, du cadre de maîtrise des risques** (qualité des contrôles), de mesures prospectives, l'analyse des causes racines.
  - Le processus d'analyse de scénarios pourrait être utilisé pour identifier différentes hypothèses ainsi que leurs conséquences (en termes d'impact notamment, la fréquence étant a priori faible) en complément d'autres outils basés sur des données historiques ou des évaluations actuelles des risques. Il pourrait également être intégré aux plans de reprise après sinistre et de continuité des activités afin d'être utilisé dans le cadre des tests de résilience opérationnelle.
  - Compte tenu de la subjectivité du processus de scénario, il est important de **mettre en place un cadre de gouvernance solide et une revue indépendante** pour garantir l'intégrité et la cohérence du processus.
- **Benchmark et analyse comparative**
  - Le benchmark et l'analyse comparative consistent à exploiter différents outils de mesure et de gestion des risques déployés au sein de la banque, ainsi que des comparaisons des résultats de ces différents outils de mesure et de gestion des risques avec celles d'autres établissements avec des activités similaires.
  - Ces comparaisons[8] peuvent notamment être effectuées pour améliorer la compréhension du profil de risque opérationnel de la banque. Par exemple, la comparaison de la fréquence et de la gravité des pertes internes avec les auto-évaluations peut aider la banque à déterminer si ses processus d'auto-évaluation fonctionnent efficacement.

[8] La Direction des risques opérationnels compare ainsi les cartographies des différentes entités au sein d'un groupe qui ont des activités similaires, met en place des approches transverses sur certains risques portés par la plupart des activités etc.

        - Les données des scénarios peuvent être comparées aux données de pertes internes et externes pour mieux comprendre la gravité de l'exposition de la banque à des événements de risque potentiels.
- Les banques doivent s'assurer que les résultats des outils d'évaluation du risque opérationnel sont :
    - Fondés sur des données exactes, dont l'intégrité est assurée par une gouvernance forte et des procédures de vérification et de validation solides ;
    - **Pris en compte de manière adéquate dans les mécanismes internes de tarification et de mesure des performances** ainsi que pour les évaluations des opportunités commerciales ; et
    - Font l'objet de plans d'action ou de plans de remédiation contrôlés par le CGRO lorsque cela est nécessaire.
- **Ces outils d'évaluation du risque opérationnel peuvent également contribuer directement à l'approche de la résilience opérationnelle** d'une banque, en particulier les procédures de gestion des événements, d'auto-évaluation et d'analyse de scénarios, car ils permettent aux banques d'identifier et de surveiller les menaces. En effet, ces outils permettent aux banques d'identifier et de surveiller les menaces et les vulnérabilités de leurs opérations critiques.
    - Les résultats de ces outils constituent des opportunités d'amélioration des contrôles et des procédures de résilience opérationnelle, comme l'indiquent les Principes pour la résilience opérationnelle du Comité[9].

Principe 7 : Les instances dirigeantes doivent s'assurer que le processus de gestion du changement facilite la prise en compte du risque opérationnel, que ce processus est approprié, doté de ressources appropriées et articulé de manière adéquate entre les différentes lignes de défense concernées[10].

- En général, l'exposition au risque opérationnel d'une banque évolue lorsque la banque développe de nouvelles activités ou développe de nouveaux produits ou services ; pénétrer sur des marchés ou des juridictions avec lesquelles la banque n'a pas l'habitude de travailler ; mise en œuvre de processus opérationnels ou de systèmes technologiques nouveaux ou modifiés, et/ou l'engagement dans des activités géographiquement éloignées du siège social.
    - **La gestion du changement doit prendre en compte l'évolution des risques associés** dans le temps, du début à la fin (par exemple, tout au long du cycle de vie d'un produit).
- Une banque devrait disposer de politiques et de procédures définissant le processus d'identification, de gestion, de **validation, d'approbation et de suivi des changements sur la base de critères objectifs défini.**
    - La mise en œuvre des changements devrait être suivie par des contrôles de suivi spécifiques. Les politiques et procédures de gestion du changement doivent faire l'objet d'un examen et d'une mise à jour indépendants et réguliers.
- **Responsabilités conformément au modèle des trois lignes de défense**, en particulier :
    - **La première ligne de défense doit procéder à des évaluations du risque opérationnel et du contrôle des nouveaux produits**, activités, processus et systèmes nouveaux, y compris l'identification et l'évaluation du changement nécessaire au

[9] Principles for operational resilience, March 2021.BIS

[10] Il s'agit là d'intégrer très en amont le risque opérationnel dans la gestion de projet afin d'anticiper les effets potentiels des projets sur le profil de risque de l'établissement et de prendre éventuellement des mesures adaptées de maîtrise des risques et de pilotage (*Ndt*).

cours des phases de décision et de planification des évolutions **jusqu'à la mise en œuvre et le suivi une fois la mise en œuvre effective**.
    - La deuxième ligne de défense (CGRO) doit challenger les évaluations des risques et les contrôles opérationnels effectuées par la première ligne de défense, et suivre la mise en œuvre des contrôles ou des mesures correctives appropriés.
    - **Le CGRO[11] doit couvrir toutes les phases de ce processus**. En outre, le CGRO doit s'assurer que tous les fonctions concernés (par exemple, les finances, la conformité, le juridique, les métiers opérationnels, les TIC, la gestion des risques) sont impliqués de manière appropriée.
- Une banque devrait disposer de politiques et de procédures pour l'examen et l'approbation de nouveaux produits, activités, processus et systèmes nouveaux. Le processus d'examen et d'approbation devrait prendre en compte les éléments suivants :
    - **Les risques inhérents** - y compris les risques juridiques, de TIC et de modèle - au lancement de nouveaux produits, services, activités et opérations sur des nouveaux marchés, ainsi que dans la mise en œuvre de nouveaux processus, compétence et de systèmes (en particulier lorsqu'ils sont externalisés).
    - **Les modifications du profil de risque opérationnel**, **de l'appétit et de la tolérance de la banque**, y compris les modifications du risque des produits ou activités existants.
    - **Les contrôles nécessaires**, les processus de gestion des risques et les stratégies d'atténuation des risques.
    - Le risque résiduel.
    - **Les modifications apportées aux seuils ou limites** de risque pertinents.
    - Les procédures et les paramètres permettant d'évaluer, de surveiller et de gérer le risque des nouveaux produits et services, activités, marchés, juridictions, processus et systèmes.
- Le processus d'examen et d'approbation doit permettre de s'assurer qu'un investissement approprié a été réalisé en matière de ressources humaines et d'infrastructure technologique avant que le projet ne soit lancé.
    - **Les changements doivent être surveillés, pendant et après leur mise en œuvre**, afin d'identifier toute évolution importante par rapport au profil de risque opérationnel prévu et de gérer tout risque potentiel.
- **Les banques doivent, dans la mesure du possible, tenir un référentiel central (registre) de leurs produits et services (y compris ceux qui sont externalisés)** afin de faciliter le suivi des changements.

3.2. Pilotage et reporting

Principe 8 : La direction générale doit mettre en place un processus de suivi régulier des profils de risque opérationnel et des expositions opérationnelles importantes. Des circuits d'information et de communication appropriés doivent être mis en place au niveau du conseil, des instances dirigeantes et du management opérationnel afin de contribuer à une gestion proactive du risque opérationnel.

- **Une banque doit veiller à ce que les reporting soient complets, précis, cohérents** et exploitables au sein de toutes les lignes métiers et toutes les activités/produits.
    - La première ligne de défense devrait assurer le reporting de tous les risques opérationnels résiduels, y compris les événements liés au risque opérationnel (pertes et incidents), les dysfonctionnements de contrôle, les inadéquations de processus et le non-respect des limites mis en place.

[11] CGRO : Cadre de Gestion du risque opérationnel

- Les reporting[12] doivent être gérables en termes de mise en œuvre, de fréquence et donner une visibilité sur le profil de risque opérationnel de la banque et sur le respect de la déclaration d'appétence et de tolérance au risque opérationnel.
- L'excès d'information peut perturber l'efficacité de ces reporting ainsi que le défaut dans la fiabilité ou la disponibilité des données.
- Les reporting doivent être établis **en temps utile** et une banque doit être en mesure de produire des reporting y compris dans des situations tendues (exemple : crise économique, sanitaire, politique)
- **La fréquence des reporting** doit refléter les risques encourus ainsi que le rythme et la nature des changements dans l'environnement opérationnel.
- Les résultats des activités de pilotage doivent être intégrés dans les reporting réguliers de la direction et du conseil, tout comme les évaluations du CGRO réalisées par les fonctions d'audit interne/externe et/ou de gestion des risques.
- Les reporting produits par ou pour les autorités de supervision ou pour leur compte doivent également être communiqués en interne à la direction générale et au conseil, le cas échéant.

- Les reporting sur le risque opérationnel devraient décrire le profil de risque opérationnel de la banque **en fournissant des indicateurs internes financiers, opérationnels et de conformité, ainsi que des informations externes sur le marché ou l'environnemen**t externes, informations de nature à influer sur la prise de décision.
- Les reporting sur le risque opérationnel doivent comprendre :
  - Les infractions à l'appétit pour le risque et à la déclaration de tolérance de la banque, ainsi qu'aux seuils, limites ou exigences qualitatives.
  - Des échanges et une évaluation des risques clés et émergents.
  - Des analyses des événements et pertes internes récents et significatifs liés au risque opérationnel (y compris l'analyse des causes racines).
  - Les événements externes pertinents, les évolutions réglementaires ou tout autre élément de nature à générer des conséquences négatives pour la banque.
- Les processus de saisie des données et de reporting des risques doivent être analysés périodiquement afin d'améliorer la performance de la gestion des risques ainsi que d'améliorer les politiques, procédures et pratiques de gestion des risques.

3.3. Contrôle et dispositif d'atténuation des risques

Principe 9 : Les banques doivent disposer d'un environnement de contrôle solide qui utilise des politiques, des processus et des systèmes, des contrôles internes appropriés et des stratégies appropriées d'atténuation et/ou de transfert des risques.

- Les contrôles internes doivent être conçus de manière à fournir une assurance raisonnable que la banque gèrera ses opérations de manière efficace et efficiente, réussira à protéger ses actifs, à produire des reporting financiers fiables et à se conformer aux lois et règlements applicables.
- Un programme adapté de contrôle interne se compose de quatre éléments qui font partie intégrante du processus de gestion des risques[13] :
  - Evaluation des risques,
  - Activités de contrôle,
  - Information et communication,

[12] Se référer également au BCBS 239 (https://www.bis.org/publ/bcbs239.pdf)
[13] Cf. Gestion ERM COSO (https://www.coso.org/Documents/COSO-ERM-Executive-Summary-French.pdf)

- Activités de suivi (pilotage et surveillance).

- Les processus et procédures de contrôle doivent inclure un système permettant de garantir la conformité aux politiques, règlements et lois.
- **Voici quelques exemples des principaux éléments d'une évaluation de la conformité aux politiques :**
  - Evaluation au plus haut niveau des avancée par rapport aux objectifs fixés.
  - Vérification de la conformité aux processus de contrôle.
  - Revue du traitement et de la résolution des cas de non-conformité.
  - Evaluation des validations et autorisations requises pour assurer le respect des niveaux de responsabilité à un niveau de gestion approprié.
  - Suivi des reporting relatifs aux dérogations approuvées par rapport aux seuils ou aux limites (exemple : justification de dépassement de limites ou des règles de délégation), aux dérogations de la direction et à d'autres écarts par rapport à la politique, aux règlements et à la réglementation.
- Les processus et procédures de contrôle devraient traiter de la manière dont la banque s'assure que la résilience opérationnelle est maintenue à la fois dans des circonstances normales et en cas de crise, reflétant la diligence raisonnable menée par les différentes fonctions concernées, conformément au dispositif mis en place par la banque en matière de résilience opérationnelle.
- **Un environnement de contrôle efficace suppose également une séparation appropriée des fonctions.**
  - Le principe de séparation des tâches, les règles des 4-yeux sont des éléments importants d'un environnement de contrôle efficace.
  - Un processus qui fait appel à deux ou plusieurs entités distinctes (généralement des personnes) opérant de concert pour protéger des fonctions ou des informations sensibles) ou d'autres contre-mesures, peuvent entraîner la dissimulation de pertes, d'erreurs ou d'autres actions inappropriées.
  - C'est pourquoi les domaines dans lesquels des conflits d'intérêts peuvent survenir doivent être identifiés, réduits au minimum et faire l'objet d'une surveillance et d'un examen indépendants attentifs.
- **Outre la séparation des tâches et le contrôle 4 yeux, les banques doivent veiller à ce que d'autres mesures de traçabilité soient mises en place**.
  - D'autres contrôles internes sont également en place, le cas échéant, pour faire face au risque opérationnel. Voici quelques exemples de ces contrôles :
  - Des règles de délégation et/ou des processus d'approbation clairement établis ;
  - Une surveillance efficace du respect des seuils ou limites de risque attribués ;
  - La mise en place de dispositifs de sécurité concernant l'accès aux actifs et aux dossiers bancaires (notamment dossiers client) et à leur utilisation ;
  - Des ressources et un niveau de compétence adaptés afin de maintenir l'expertise technique nécessaire à la réalisation et au suivi des contrôles ;
  - Processus permanents d'identification des unités commerciales ou des produits dont les rendements semblent ne pas correspondre aux attentes raisonnables ;
  - Vérification et rapprochement réguliers des transactions et des comptes ;
  - Gestion des congés prévoyant que les dirigeants et les employés s'absentent de leurs fonctions pendant une période d'au moins deux semaines consécutives.
- L'utilisation efficace et la mise en œuvre de technologie peuvent contribuer à l'environnement de contrôle.

  - Par exemple, les processus automatisés sont moins sujets à erreur que les processus manuels. Cependant, les processus automatisés présentent des risques qui doivent être traités par une bonne gouvernance des risques IT et des programmes de gestion des risques liés à l'infrastructure informatique.
- **L'utilisation de produits, d'activités, de processus et de canaux de distribution liés à la technologie expose la banque à un risque opérationnel** et à la possibilité de pertes financières importantes.
  - C'est pourquoi la banque devrait mettre en place un dispositif d'identification, de mesure, de surveillance et de gestion des risques liés aux technologiques selon les mêmes principes que la gestion du risque opérationnel traditionnel.
- Si le recours à des entités externes, dont les prestataires de services dans le cadre de l'externalisation, peut aider à gérer les coûts, fournir une expertise, étendre les offres de produits et améliorer les services, ce recours introduit également des risques que les instances dirigeantes doivent prendre en compte.
  - **Le conseil et la direction générale ont la responsabilité de comprendre les risques opérationnels liés à l'externalisation** et s'assurer que des politiques et des pratiques efficaces de gestion des risques sont en place pour gérer le risque lié aux activités externalisées.
- De plus, il est important de prendre en compte le risque de concentration lié à l'externalisation ains que la complexité de certaines externalisations. Les politiques en matière de risques liés aux tiers (dans le cadre des politiques du CGRO) et les activités de gestion des risques devraient comprendre :
  - Des procédures pour déterminer si les activités peuvent être externalisées et de quelle manière ;
  - Des processus de diligence raisonnable dans la sélection des prestataires de services potentiels ;
  - **Une gestion adaptée des contrats, intégrant notamment la propriété et la confidentialité des données, ainsi que les droits de résiliation**.
  - Des programmes de gestion et de surveillance des risques associés à l'accord d'externalisation, incluant le suivi de la situation financière du prestataire de services ;
  - La mise en place **d'un environnement de contrôle efficace** au sein de la banque et du prestataire de services, qui doit inclure **un registre des activités externalisées,** des mesures et des reporting pour faciliter la surveillance du prestataire de services.
  - L'élaboration de plans d'urgence et de continuité viables ;
  - L'exécution de contrats complets et/ou d'accords de niveau de service avec une répartition claire des responsabilités entre le prestataire de services externalisés et la banque ;
  - Accès des autorités de contrôle et de résolution des banques (exemple ACPR en France) chez le prestataire.

- Ainsi disposer de contrôles inadaptés face au risque de l'externalisation n'est pas une option envisageable.
  Les instances dirigeantes peuvent compléter le dispositif en transférant une partie du risque à une tierce partie, par exemple par une assurance.
  - Le conseil doit déterminer l'exposition maximale aux pertes que la banque est disposée à tolérer et sa capacité financière d'assumer la perte. Il doit également

procéder à un examen annuel du programme de gestion des risques et des assurances de la banque. Si les besoins spécifiques d'une banque doivent être déterminés sur une base individuelle, de nombreuses juridictions ont des exigences réglementaires qui doivent être prises en compte.

- Le transfert de risque étant un substitut imparfait à de solides contrôles et des programmes de gestion des risques, **les banques doivent considérer les outils de transfert de risque comme un complément plutôt que comme un substitut** d'un cadre de contrôle interne pertinent.
    - La mise en place de mécanismes permettant d'identifier, de reconnaître et de rectifier rapidement des erreurs liées au risque opérationnel - ou une exposition à un risque juridique spécifique - peut réduire considérablement les expositions.
    - Il convient également **d'examiner attentivement dans quelle mesure les outils d'atténuation des risques tels que les assurances réduisent réellement le risque**, transfèrent le risque à un autre secteur ou domaine d'activité, **ou créent un nouveau risque** (par exemple, le risque de contrepartie).
- Les banques devraient disposer d'une classification, d'une méthodologie et de procédures harmonisées de gestion du risque opérationnel établies par le CGRO.

4. Technologies de l'information et de la communication

Principe 10 : les banques doivent mettre en œuvre un solide programme de gestion du risque lié aux TIC[14] , aligné sur leur cadre de gestion du risque opérationnel.

- L'efficacité et la sécurité des TIC sont primordiales pour qu'une banque puisse exercer correctement ses activités.
    - L'utilisation et la mise en œuvre appropriées d'une bonne gestion des risques liés aux TIC contribuent à l'efficacité de l'environnement de contrôle et sont fondamentales pour la réalisation des objectifs stratégiques d'une banque.
    - La banque doit s'assurer que ses TIC soutiennent et facilitent pleinement ses opérations. **La gestion des risques liés aux TIC devrait réduire l'exposition d'une banque au risque opérationnel** lié aux pertes directes, aux actions en justice, à l'atteinte à la réputation, aux perturbations des TIC et à l'utilisation abusive de la technologie, conformément à son appétit pour le risque et à sa déclaration de tolérance.
- **La gestion des risques liés aux TIC comprend** :
    - L'identification et l'évaluation des risques liés aux TIC.
    - Des mesures d'atténuation des risques liés aux TIC conformes au niveau de risque évalué (par exemple, cybersécurité, programmes de réponse et de récupération, processus de gestion du changement des TIC, gestion des incidents liés aux TIC, (y compris la transmission en temps utile des informations pertinentes aux utilisateurs).
    - Suivi de ces mesures d'atténuation (y compris des tests réguliers)
    - **Pour assurer la confidentialité, l'intégrité et la disponibilité des données** et des systèmes, le conseil devrait régulièrement superviser l'efficacité de la gestion des risques liés aux TIC de la banque et les instances délibérantes devrait évaluer régulièrement la

[14] Les "technologies de l'information et de la communication" désignent la conception physique et logique sous-jacente des technologies de l'information et de communication, les différents composants matériels et logiciels, les données et les environnements d'exploitation.

conception, la mise en œuvre et l'efficacité de la gestion des risques liés aux TIC de la banque.

  - Les stratégies commerciales, de gestion des risques et de TIC doivent être alignées afin de respecter l'appétit pour le risque et la déclaration de tolérance de la banque, ainsi que le respect des obligations en matière de protection de la vie privée et les autres lois applicables.
  - Les banques doivent surveiller en permanence leurs TIC et rendre compte régulièrement compte à la direction générale des risques, des contrôles et des événements liés aux TIC.
  - Les risques, les contrôles et les événements liés aux TIC.

- La gestion des risques liés aux TIC et les processus complémentaires mis en place par les banques devraient :
  - Être examinés régulièrement pour vérifier leur exhaustivité par rapport aux normes et aux meilleures pratiques du secteur, ainsi que par rapport à l'évolution des menaces (par exemple, la cybercriminalité) et des technologies nouvelles ou en évolution ;
  - Être régulièrement testé dans le cadre d'un programme visant à identifier les écarts par rapport aux objectifs de tolérance aux risques fixés et à faciliter l'amélioration du système d'identification, de protection, de détection et de gestion des risques liés aux TIC
  - Utiliser des renseignements exploitables pour améliorer en permanence leur connaissance de la situation en ce qui concerne les points suivants : vulnérabilités des systèmes, réseaux et applications TIC et faciliter la prise de décision efficace dans la gestion des risques ou du changement
- Les banques devraient élaborer des approches de la préparation aux TIC pour les scénarios de stress résultant d'événements externes tels que la nécessité de faciliter la mise en œuvre d'un accès à distance à grande échelle, le déploiement rapide d'actifs physiques et/ou l'expansion significative de la bande passante pour prendre en charge les connexions des utilisateurs à distance et la protection des données des clients.
- Les banques doivent s'assurer que :
  - Des stratégies appropriées d'atténuation des risques sont élaborées pour les risques potentiels associés à une interruption ou à la compromission des systèmes, réseaux et applications TIC. Les banques doivent évaluer si les risques, pris conjointement avec ces stratégies, s'inscrivent dans le cadre de l'appétit pour le risque et de la tolérance au risque de la banque.
  - Des processus bien définis pour la gestion des utilisateurs privilégiés et le développement des applications sont en place ; et
  - Des mises à jour régulières sont apportées aux TIC, y compris à la cybersécurité, afin de maintenir un dispositif de sécurité approprié.

5. La continuité des activités

Principe 11 : Les banques doivent mettre en place des plans de continuité des activités afin de garantir leur capacité à fonctionner sur une base continue et limiter les pertes en cas de perturbation grave de l'activité.

- Les plans de continuité d'activité doivent être liés au cadre de gestion du risque opérationnel de la banque.

- **Une gouvernance saine et efficace de la politique de continuité d'activité des banques requiert** :
    - Un examen et une approbation réguliers par le conseil.
    - Une forte implication de la direction générale et des responsables des unités opérationnelles dans sa mise en œuvre.
    - L'engagement des première et deuxième lignes de défense dans sa conception.
    - Un examen régulier par la troisième ligne de défense.
- Les banques doivent préparer des plans de continuité d'activité (PCA) prospectifs avec des analyses de scénarios associées à des évaluations d'impact pertinentes et des procédures de reprise pertinentes :
- Une banque devrait fonder sa politique de continuité d'activité sur des analyses de scénarios de perturbations potentielles qui identifient et classent les opérations commerciales critiques et les principales dépendances. Par ailleurs, **les banques devraient couvrir toutes leurs unités opérationnelles ainsi que les fournisseurs critiques et les principaux tiers (banques centrales, chambre de compensation, etc.).**
    - Chaque scénario doit faire l'objet d'une évaluation d'impact quantitative et qualitative ou d'une analyse d'impact (Business Impact Analysis – BIA) afin d'évaluer les conséquences financières, opérationnelles, juridiques et de réputation.
    - Les scénarios de stress doivent faire l'objet de seuils ou de limites (tels que l'interruption maximale tolérable) pour l'activation d'une procédure de continuité des activités. La procédure doit aborder
- Les aspects liés à la reprise, fixer des objectifs de temps de rétablissement (RTO) et des objectifs de point de rétablissement (RPO), ainsi que des directives de communication pour informer la direction, les employés, les autorités de régulation, les clients, les fournisseurs et, le cas échéant, les autorités.
- **Une banque devrait revoir périodiquement ses plans et politiques de continuité d'activité** pour s'assurer que, les stratégies d'urgence restent cohérentes avec les opérations, risques et menaces actuels.
- **Les programmes de formation et de sensibilisation devraient être personnalisés** en fonction des rôles spécifiques afin de garantir que le personnel puisse effectivement exécuter les plans d'urgence.
- Les procédures de continuité des activités doivent être **testées périodiquement** pour s'assurer que les objectifs et les délais de reprise et de rétablissement peuvent être respectés. Dans la mesure du possible, **une banque devrait participer aux tests de continuité d'activité avec les principaux prestataires de services**. Les résultats des activités formelles de test et de révision devraient être **communiqués à la direction générale et au conseil**.

6. Rôle de la communication

Principe 12 : Les informations publiées par une banque devraient permettre aux parties prenantes d'évaluer son approche de la gestion du risque opérationnel et son exposition à ce risque.

- La communication au public par une banque d'informations pertinentes sur la gestion du risque opérationnel peut conduire à plus de transparence et le développement de meilleures pratiques dans le secteur grâce à la discipline de marché.

- **Le volume et le type d'informations publiées devraient être proportionnels à la taille, au profil de risque** et à la complexité des opérations d'une banque, ainsi qu'à l'évolution des pratiques du secteur.
    - Les banques doivent divulguer à leurs parties prenantes des informations pertinentes sur l'exposition au risque opérationnel (y compris les pertes opérationnelles significatives), tout en évitant de créer un risque opérationnel par cette divulgation (par exemple, description de vulnérabilités de contrôle qui n'auraient pas été traitées).
    - Une banque devrait divulguer son dispositif de gestion du risque opérationnel d'une manière qui permette aux parties prenantes de déterminer si la banque est en mesure d'atteindre ses objectifs, si la banque identifie, évalue, surveille et contrôle/atténue efficacement le risque opérationnel.
- **Les banques devraient disposer d'une politique de communication formelle**, **soumise à un examen et à une approbation régulière et indépendante** de la direction générale et du conseil.
    - Cette politique doit aborder l'approche de la banque pour déterminer les informations sur le risque opérationnel qu'elle publiera et les dispositifs de contrôle associés au processus de publication.
    - En outre, les banques doivent mettre en œuvre un processus d'évaluation de la pertinence de leurs informations et de leur politique de communication.

7. Rôle des autorités de supervision

- Les autorités de contrôle devraient évaluer régulièrement le dispositif de gestion du risque opérationnel des banques en évaluant leurs politiques, processus et systèmes liés au risque opérationnel.
    - Les autorités de contrôle doivent s'assurer que des mécanismes appropriés sont en place pour leur permettre de mettre à jour si nécessaire en fonction de l'évolution du risque opérationnel des banques.
- **Les évaluations prudentielles du risque opérationnel doivent porter sur tous les domaines décrits dans les Principes de bonne gestion du risque opérationnel**.
    - Lorsque les banques font partie d'un groupe financier, les autorités de contrôle devraient s'assurer que des processus sont en place pour garantir que le risque opérationnel est géré de manière appropriée et intégrée au sein du groupe.
    - Lors de l'évaluation du dispositif CGRO des banques, la coopération et l'échange d'informations avec d'autres autorités de contrôle, conformément aux procédures établies, peuvent être nécessaires.
    - Dans certaines circonstances, les autorités de contrôle peuvent choisir de faire appel à des auditeurs externes dans le cadre de ces processus d'évaluation.
- **Les superviseurs devraient prendre des mesures pour s'assurer que les banques remédient aux déficiences identifiées lors de l'examen prudentiel** des CGRO des banques. Les autorités de contrôle devraient utiliser les outils les plus adaptés aux circonstances particulières des banques et à leur environnement opérationnel.
- Pour s'assurer que les superviseurs reçoivent des informations actualisées sur le risque opérationnel, les autorités de contrôle peuvent souhaiter mettre en place des mécanismes de reporting directement avec les banques et les auditeurs externes (par exemple, les reporting internes de la direction des banques sur le risque opérationnel pourraient être mis à la disposition des autorités de contrôle).

Les superviseurs devraient encourager les efforts de développement au sein des établissements quant à la gestion du risque opérationnel en suivant, en comparant et en évaluant les améliorations récentes et les plans de développement futur des banques.