12

RISQUES OPÉRATIONNELS

12.1 Politique de risques opérationnels 244

Organisation 244
Méthodologie 244
Pilotage des risques opérationnels 245

12.2 Surveillance 246

Collecte des incidents et des pertes 246
Suivi des risques opérationnels 246
Procédure d'alerte pour les incidents 246
Mesure du risque opérationnel 246

12.3 Contrôle 247

Techniques de réduction du risque opérationnel 248

12.1 Politique de risques opérationnels

Le Groupe BPCE s'est muni d'un dispositif de mesure des risques non financiers *via* l'utilisation normalisé d'indicateurs. Ceux-ci couvrent les indicateurs du dispositif RAF, les indicateurs issus de l'arrêté du 3 novembre 2014, mais aussi d'indicateurs qualitatifs visant à mesurer l'adhérence de la filière aux normes du risque opérationnel.

La politique risques opérationnels du Groupe consiste à conserver, par entité et en consolidé, l'ensemble de ces indicateurs sous les limites fixées. En cas de dépassement, des mesures appropriées et actions correctives doivent être engagées par les métiers propriétaires des risques pour remédier aux éventuelles défaillances. Ces mesures et actions correctives doivent être suivies par le comité en charge des risques opérationnels.

La politique risques opérationnels fait l'objet d'une révision annuelle par le comité dédié.

Organisation

Au sein de la direction des Risques du Groupe BPCE, le département des risques opérationnels Groupe (DROG) est en charge de l'identification, de la mesure, du suivi et de la maîtrise des risques opérationnels auxquels toutes les activités et fonctions des établissements et filiales sont exposées.

Le dispositif risque opérationnel est articulé autour :

- d'une organisation centrale et d'un réseau de responsables risques opérationnels et de correspondants risques opérationnels, déployé au sein de toutes les activités, entités et filiales des établissements et filiales du Groupe ;
- d'une méthodologie, reposant sur des référentiels et un outil communs pour l'ensemble du Groupe.

La filière risques opérationnels intervient :

- sur l'ensemble des structures consolidées ou contrôlées par l'établissement ou la filiale (bancaires, financières, assurances…) ;
- sur l'ensemble des activités comportant des risques opérationnels, y compris les activités externalisées au sens de l'article 10 q et de l'article 10 r de l'arrêté du 3 novembre 2014 modifié « activités externalisées et prestations de services ou autres tâches opérationnelles essentielles ou importantes ».

Le comité des risques non financiers Groupe (CRNFG) définit la politique des risques déployée au sein des établissements et filiales, et le DROG en contrôle l'application dans le Groupe.

Méthodologie

Le dispositif de gestion des risques opérationnels s'inscrit dans les dispositifs Risk Assessment Statement (RAS) et Risk Assessment Framework (RAF) définis par le Groupe. Ces dispositifs et indicateurs sont déclinés aux bornes de chaque établissement et filiale du Groupe.

La méthodologie de cartographie s'inscrit dans le dispositif de contrôle permanent du Groupe et intègre les filières risques opérationnels, conformité, sécurité du système d'Information, sécurité des personnes et des biens et enfin contrôles permanents.

La mesure de l'exposition aux risques est fondée sur un modèle prospectif permettant de quantifier et classer les situations de risques et fournir ainsi au comité dédié risques non financiers les éléments qui lui permettront de définir sa tolérance aux risques.

Les indicateurs prédictifs de risques sont issus des principaux risques identifiés dans la cartographie des risques non financiers.

La surveillance et le suivi des risques sont renforcés par la production de reportings destinés à livrer une mesure harmonisée à l'ensemble du Groupe de son exposition et du coût du risque.

La production de la filière RO effectue deux types de contrôles de niveau 2 sur les risques opérationnels (ces contrôles permanents de niveau 2 seront réalisés à partir de fin 2022 par le département Gouvernance et contrôle des risques de la DRG) :

- des contrôles exhaustifs et automatiques ;
- des contrôles par échantillon et manuels.

La fonction risques opérationnels de BPCE s'assure que l'organisation et les dispositifs en place au sein des établissements et des filiales leur permettent d'atteindre leurs objectifs et de remplir leurs missions.

À ce titre, elle :

- exerce une mission générale d'animation de la filière et un rôle de surveillance et de contrôle des risques sur les établissements/filiales et leurs filiales ;
- centralise et analyse l'exposition du Groupe aux risques non financiers, contrôle la mise en œuvre des actions correctrices décidées en comité en charge des risques opérationnels et escalade les délais excessifs de mise en œuvre ;
- exerce des contrôles afin de s'assurer du respect des normes et méthodes déployées dans les établissements et filiales ;
- assure la veille réglementaire, diffuse et relaie les alertes risques opérationnels dues aux incidents propageables aux établissements/filiales concernés ;
- établit des reportings, par établissement ou filiale, Groupe et réglementaires (COREP RO), analyse les reportings et contenus des comités dédiés des établissements et filiales et alerte le comité risques non financiers Groupe en cas de dispositif défaillant et/ou d'exposition aux risques excessive, qui lui-même se charge d'alerter l'établissement.

Pilotage des risques opérationnels

Le pilotage des risques opérationnels dans le Groupe est coordonné à deux niveaux :

1. Au niveau de chaque établissement du Groupe	2. Au niveau du Groupe BPCE
Le comité en charge des risques opérationnels s'assure de la déclinaison de la politique de maîtrise des risques opérationnels et s'assure de la pertinence et de l'efficacité du dispositif. À ce titre, il : • prend connaissance des incidents majeurs et récurrents et valide les actions correctives à mener ; • prend connaissance des indicateurs en dépassement, décide des actions correctives à mener et effectue le suivi de l'état d'avancement des actions de réductions des risques ; • examine les contrôles permanents réalisés au titre de la filière risques opérationnels et notamment les délais excessifs de mise en œuvre des actions correctives ; • contribue à l'organisation et à la formation du réseau des correspondants risque opérationnel ; • exprime les éventuels besoins d'évolution des polices d'assurance locales. • sa fréquence varie en fonction de l'intensité du risque de l'établissement, selon trois régimes de fonctionnement revus annuellement par le CRNFG et communiqués aux entités.	De fréquence trimestrielle, le comité des risques non financiers du Groupe (CRNFG) est présidé par un membre du comité de direction générale. Le comité a pour principales missions de définir la norme RO et s'assurer du déploiement du dispositif RO au sein des entités du Groupe et de définir la politique RO du Groupe. À ce titre, il : • examine les risques majeurs du Groupe et définit son niveau de tolérance, décide la mise en œuvre des actions correctives globales affectant le Groupe et en suit les progrès ; • évalue le niveau de ressources à allouer ; • passe en revue les incidents majeurs sur le périmètre, valide la cartographie des risques opérationnels agrégée au niveau Groupe qui contribue à la macrocartographie des risques ; • suit les situations de risques majeures sur toutes les activités du Groupe intégrant les risques de non-conformité, du domaine de révision finance, de la sécurité des biens et personnes, PUPA, de la sécurité financière et de la sécurité des systèmes d'information (SSI) ; • enfin, il valide les indicateurs RAF Groupe liés aux risques non financiers ainsi que leurs seuils.

12.2 Surveillance

Collecte des incidents et des pertes

La collecte des incidents répond à un objectif de connaissance du coût du risque, d'amélioration permanente des dispositifs de contrôle et à des objectifs réglementaires.

La constitution d'un historique des incidents (base incident) a pour objectif de :

- disposer d'une profondeur d'analyse et d'une courbe d'expérience pour adapter les plans d'action et évaluer leur pertinence ;
- produire les états réglementaires semestriels risques opérationnels du COREP ;
- produire des reportings à destination des organes exécutifs et délibérants et à destination des opérationnels ;
- disposer d'un historique applicable dans le cadre d'une modélisation du risque opérationnel.

La déclaration des incidents est faite au fil de l'eau, dès leur détection, selon le dispositif Groupe. Une procédure d'alerte pour incident jugés graves et dépassant des seuils internes vient compléter le dispositif de collecte.

Suivi des risques opérationnels

CARTOGRAPHIE

Le dispositif de gestion du risque opérationnel s'appuie sur un processus de cartographie mis à jour annuellement par l'ensemble des entités du Groupe.

La démarche de cartographie permet d'identifier et de mesurer de façon prospective les processus les plus sensibles. Elle permet, pour un périmètre donné, de mesurer l'exposition aux risques des activités du Groupe pour l'année à venir. Cette exposition est alors évaluée et validée par les comités concernés afin de déclencher des plans d'action visant à réduire l'exposition. Le périmètre de cartographie inclut les risques émergents, les risques liés aux technologies de l'information et de la communication et à la sécurité dont cyber, les risques liés aux prestataires et les risques de non-conformité.

Cette même cartographie est utilisée dans le cadre de l'ICAAP du Groupe pour permettre d'identifier et de valoriser les risques opérationnels les plus importants du Groupe. La cartographie des risques opérationnels alimente également la macrocartographie des risques des établissements et donc, au global, du Groupe.

PLANS D'ACTION ET SUIVI DES ACTIONS DE REMÉDIATION

Les actions correctives sont engagées pour atténuer la fréquence, l'impact ou la propagation des risques opérationnels. Elles peuvent être mises en place suite à l'exercice de cartographie des risques opérationnels, de dépassement de seuil des indicateurs de risques ou à la survenance d'incidents.

L'avancement des principales actions fait l'objet d'un suivi en comité risques opérationnels de chaque entité.

Par ailleurs au niveau du Groupe, l'avancement des plans d'action des principales zones de risques fait l'objet d'un suivi spécifique en comité des risques non financiers.

Procédure d'alerte pour les incidents

La procédure d'alerte sur les incidents graves, applicable à l'ensemble du périmètre du Groupe BPCE, vise à compléter et renforcer le système de collecte des pertes au sein du Groupe.

Un incident de risque opérationnel est considéré grave lorsque l'impact financier potentiel au moment de la détection est supérieur à 300 000 euros. Est également considéré comme grave tout incident de risque opérationnel qui aurait un impact fort sur l'image et la réputation du Groupe ou de ses filiales.

Cette procédure est complétée par celle dédiée aux incidents de risques opérationnels significatifs au sens de l'article 98 de l'arrêté du 3 novembre 2014 modifié par l'arrêté du 25 février 2021, dont le seuil de dépassement minimum est fixé à 0,5 % des fonds propres de base de catégorie 1.

Mesure du risque opérationnel

Le Groupe BPCE applique la méthode standard pour le calcul des exigences en fonds propres. Au demeurant, les éléments de contrôle interne sont pris en compte dans l'évaluation des risques nets auxquels le Groupe est exposé.

12.3 Contrôle

Des Contrôles Permanents ont été définis afin de contrôler la qualité du dispositif de gestion des risques opérationnels.

Deux types de Contrôles de Niveau 2 sont opérés sur les Risques Opérationnels :

- Contrôles d'adhérence aux normes (exhaustifs et automatiques) :

Le Groupe BPCE effectue un contrôle du dispositif qui présente les écarts par rapport aux Normes Risques Opérationnels sur le périmètre des différents thèmes de la Gestion des Risques Opérationnels : Dispositif organisationnel de la gestion des RO, incidents, cartographie, indicateurs prédictifs de risques, actions correctives, etc.

- Contrôles de qualité de données (par échantillons et manuels) :

Le Groupe BPCE effectue des contrôles de niveau 2 de la filière risques opérationnels.

Ces contrôles sont effectués sur la base des rapports de contrôle du dispositif des Établissements, donc sur le même périmètre que ces rapports : dispositif, incidents, cartographie (situations de risques), indicateurs prédictifs de risques, actions correctives.

La plus large part de ces contrôles est effectuée sur la base d'échantillons de données extraites de l'outil de gestion des risques opérationnels. Les résultats de ces contrôles par échantillons de niveau 2 sont enregistrés dans l'outil de gestion des contrôles permanents.

D'autres contrôles concernent certains points ayant trait à la couverture des risques. Ils sont exhaustifs et leurs résultats font l'objet d'une formalisation spécifique (PV de réunions relatifs aux incidents graves, relevé de décisions…).

FAITS MARQUANTS

Le suivi des risques opérationnels a fait l'objet des mesures spécifiques suivantes depuis le début de la crise en Ukraine :

- mesure de l'exhaustivité des impacts : suivi conjoint entre les filières PUPA et risques opérationnels avec mode opératoire d'échanges et d'enregistrement des pertes sur risques opérationnels liées au conflit (établi dans le cadre d'audio-conférences mensuelles de la filière risques opérationnels des établissements) ;
- mise en place d'un reporting quotidien dédié aux pertes liées au conflit destiné à la BCE et aux dirigeants du Groupe BPCE (sous la responsabilité de l'équipe risques opérationnels consolidés).

En outre, dans un objectif d'amélioration de la maîtrise de nos risques, des travaux d'identification de leviers (évolution des procédures, intégration de workflow IT, renforcement de la formation…) visant à améliorer les résultats des contrôles de premier et second niveaux des risques Information Technologie et Communication ont été initiés.

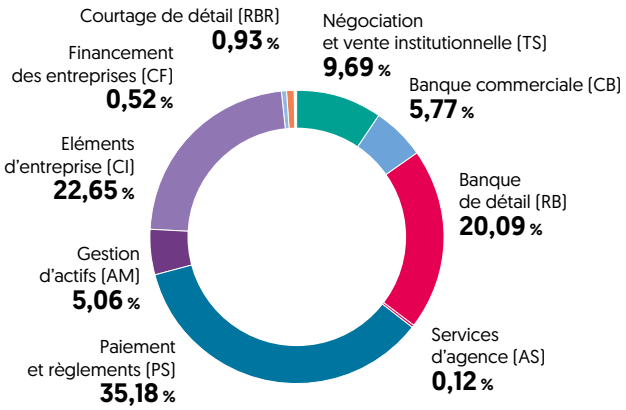
En matière d'assurance, les réseaux et les filiales bénéficient d'une couverture de leurs risques opérationnels assurables dans le cadre des polices d'assurance Groupe souscrites auprès de compagnies d'assurances de premier plan. En complément de ce dispositif, une société de réassurance interne au Groupe a été mise en place.

EU OR1 – EXIGENCES DE FONDS PROPRES POUR RISQUE OPÉRATIONNEL ET MONTANTS DES EXPOSITIONS PONDÉRÉS

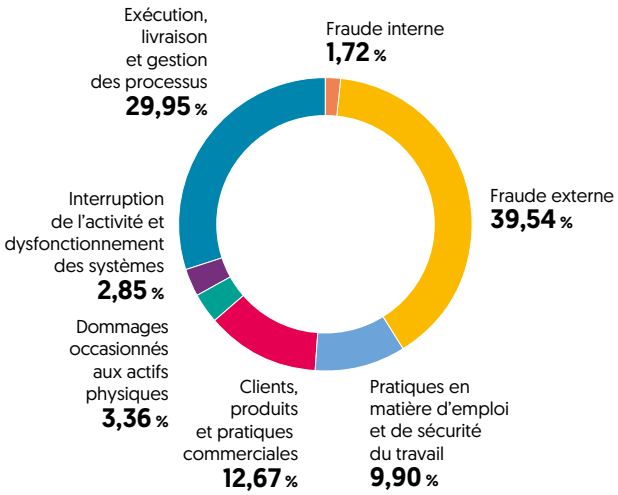
		a	b	c	d	e
		Indicateur pertinent			Exigences de fonds propres	Montant d'exposition au risque
	Activités bancaires	31/12/2020	31/12/2021	31/12/2022		
1	Activités bancaires en approche élémentaire (BIA)	-	-	-	-	-
2	Activités bancaires en approche standard (TSA)/en approche standard de remplacement (ASA)	21 810	25 368	25 634	3 301	41 266
3	*En approche standard (TSA) :*	*21 810*	*25 368*	*25 634*		
4	*En approche standard de remplacement (ASA) :*	-	-	-		
5	Activités bancaires en approche par mesure avancée (AMA)	-	-	-	-	-

RÉPARTITION DES PERTES AU 31/12/2022

RÉPARTITION DES PERTES PAR LIGNE DE MÉTIER BÂLOIS



RÉPARTITION DES PERTES PAR LIGNE DE CATÉGORIE BÂLOISE



Techniques de réduction du risque opérationnel

En matière d'assurance, les réseaux et les filiales bénéficient d'une couverture de leurs risques opérationnels assurables dans le cadre des polices d'assurance Groupe souscrites auprès de compagnies d'assurances de premier plan. Ce dispositif est complété par une captive de réassurance permettant d'adapter les niveaux de franchises.

COUVERTURE DES RISQUES ASSURABLES

Au 1er janvier 2022, BPCE SA a souscrit tant pour son propre compte :

- que pour celui de ses filiales, y compris GFS ;
- ainsi que des réseaux Banque Populaire et Caisse d'Epargne, à l'exception de la CASDEN Banque Populaire en ce qui concerne la couverture d'assurance « Dommages Matériels » aux Immeubles Sièges & Assimilés et à leur contenu (y compris matériels informatiques) et « pertes d'activités bancaires » consécutives, décrite ci-après au point E/ ;

Les principaux programmes d'assurance suivants en couverture de ses risques opérationnels assurables, en protection de son bilan et de son compte de résultat :

A/ Combinée « Globale de Banque (Dommages Aux Valeurs & Fraudes) » & « Responsabilité Civile Professionnelle d'une capacité indemnitaire totale de 217 millions d'euros par année d'assurance dont :

a) 92,5 millions d'euros par an, combinés « Globale de Banque/Responsabilité Civile Professionnelle/Cyber-Risques » et mobilisables en sous-jacent des montants garantis indiqués en b) et/ou c) et/ou d) ci-après ;

b) 48 millions d'euros par an (sous-limité en « Fraudes » à 35 millions d'euros par sinistre), dédiés au seul risque « Globale de Banque » ;

c) 25 millions d'euros par sinistre et par an, spécifiques au seul risque « Responsabilité Civile Professionnelle » ;

d) 51,5 millions d'euros par sinistre et par an, combinés « Globale de Banque/Responsabilité Civile Professionnelle » et mobilisables en excédent ou après épuisement des montants garantis indiqués en b) et/ou c) ci-avant ;

le sinistre unitaire d'intensité maximum indemnisable par ce montage s'élève à 100 millions d'euros au titre de la garantie « Responsabilité Civile Professionnelle » et à 100,5 millions d'euros au titre de la garantie « Fraude » en excédent des franchises applicables ;

B/ « Responsabilité Civile Intermédiations Réglementées » (en trois volets : Intermédiation Financière, Intermédiation en Assurances, Transaction/Gestion Immobilière) d'une capacité indemnitaire de 10 millions d'euros par sinistre et 13 millions d'euros par an.

C/ « Responsabilité Civile Exploitation » à hauteur de 100 millions d'euros par sinistre, complétée par une extension de garantie « RC Propriétaire Subsidiaire »/« RC Après Livraison – Réception » jusqu'à concurrence de 35 millions d'euros par sinistre et par année d'assurance.

D/ « Responsabilité Civile des Dirigeants et Mandataires Sociaux », à concurrence de 150 millions d'euros par sinistre et par année d'assurance.

E/ « Dommages Matériels » aux Immeubles Sièges & Assimilés et à leur contenu (y compris matériels informatiques) & « pertes d'activités bancaires » consécutives, à hauteur de 300 millions d'euros par sinistre (sous-limité en « pertes d'activités bancaires » consécutives à 100 millions d'euros par sinistre et 200 millions d'euros par an).

F/ « Protection du Patrimoine Digital contre les Cyber-Risques » & « pertes d'activités bancaires » consécutives, à hauteur de 100 millions d'euros par sinistre et 156,5 millions d'euros par année d'assurance.

La territorialité de ces couvertures s'étend au monde entier, en premier risque ou en parapluie, sous réserve de certaines exceptions, principalement en matière de « Responsabilité Civile Professionnelle » où la garantie n'est pas acquise aux établissements permanents situés aux États-Unis (la couverture étant en effet souscrite localement par les implantations américaines de GFS).

Chacune des polices d'assurance visées ci-dessus est souscrite auprès de compagnies notoirement solvables sur le marché et en excédent de franchises en rapport avec la capacité de rétention du Groupe BPCE.