ECM Pilier 3

publié au 31 décembre 2022

Groupe AGPM
SANTÉ · PRÉVOYANCE · ASSURANCE · RETRAITE

Sommaire

Déclaration sur les informations publiées au titre du Pilier 3

La Direction Générale et le Conseil d'Administration sont responsables de la mise en place et du maintien d'une structure de contrôle interne efficace régissant les publications de l'établissement, y compris celles effectuées au titre du rapport Pilier III.

Dans ce cadre, j'atteste, que la société Epargne Crédit des Militaires (ECM) publie au titre du rapport Pilier III les informations requises en vertu de la Huitième partie du règlement (UE) No 575/2013 modifié ultérieurement par le règlement (UE) No 2019/876 conformément aux politiques formelles et aux procédures, systèmes et contrôles internes.

Patrice PAULET
Président du Conseil d'Administration

Ce document a pour objectif de présenter les principaux risques auxquels la société Epargne Crédit des Militaires (ECM) est exposée dans le cadre de l'exercice de ses activités et de fournir une information sur sa gestion des risques et sur ses fonds propres.

De plus, dans la mesure où ECM ne dispose d'aucun effectif salarié et où les mandataires sociaux ne sont pas rémunérés par ECM, les états liés aux rémunérations ne sont pas applicables.

Ce document répond à la fois :
- aux obligations d'information au titre du Règlement (UE) n° 575/2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement (CRR), amendé par le Règlement (UE) n° 2019/876 dit « CRR 2 » ;
- au règlement d'exécution (UE) n°2021/637 qui fournit les états/modèles de publication au titre de la huitième partie du CRR pour améliorer la comparabilité de l'information des établissements de crédits au titre du troisième pilier de l'accord du Comité de Bâle relatif à la discipline de marché ;
- à la Directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (CRD IV), amendée par la Directive (UE) n° 2019/878 dite « CRD V ».

01

LES INDICATEURS CLÉS (EU KM)

		a	e
		31/12/2022	**31/12/2021**
	Fonds propres disponibles (montants)		
1	Fonds propres de base de catégorie 1 (CET1)	10 706 229	11 047 179
2	Fonds propres de catégorie 1	10 706 229	11 047 179
3	Fonds propres totaux	10 706 229	11 047 179
	Montants d'exposition pondérés		
4	Montant total d'exposition au risque	12 406 049	13 280 773
	Ratios de fonds propres (en pourcentage du montant d'exposition pondéré)		
5	Ratio de fonds propres de base de catégorie 1 (%)	86,30 %	83,18 %
6	Ratio de fonds propres de catégorie 1 (%)	86,30 %	83,18 %
7	Ratio de fonds propres totaux (%)	86,30 %	83,18 %
	Exigences de fonds propres supplémentaires pour faire face aux risques autres que le risque de levier excessif (en pourcentage du montant d'exposition pondéré)		
EU 7a	Exigences de fonds propres supplémentaires pour faire face aux risques autres que le risque de levier excessif (%)	0,00 %	0,00 %
EU 7b	dont : à satisfaire avec des fonds propres CET1 (points de pourcentage)	0,00 %	0,00 %
EU 7c	dont : à satisfaire avec des fonds propres de catégorie 1 (points de pourcentage)	0,00 %	0,00 %
EU 7d	Exigences totales de fonds propres SREP (%)	8,00 %	8,00 %
	Exigence globale de coussin et exigence globale de fonds propres (en pourcentage du montant d'exposition pondéré)		
8	Coussin de conservation des fonds propres (%)	2,50 %	2,50 %
EU 8a	Coussin de conservation découlant du risque macroprudentiel ou systémique constaté au niveau d'un État membre (%)		
9	Coussin de fonds propres contracyclique spécifique à l'établissement (%)		
EU 9a	Coussin pour le risque systémique (%)		
10	Coussin pour les établissements d'importance systémique mondiale (%)		
EU 10a	Coussin pour les autres établissements d'importance systémique (%)		

11	Exigence globale de coussin (%)	2,50 %	2,50 %
EU 11a	Exigences globales de fonds propres (%)	10,50 %	10,50 %
12	Fonds propres CET1 disponibles après le respect des exigences totales de fonds propres SREP (%)	0,00 %	
	Ratio de levier		
13	Mesure de l'exposition totale	18 329 648	20 472 219
14	Ratio de levier (%)	58,41%	53,96%
	Exigences de fonds propres supplémentaires pour faire face aux risques de levier excessif (en pourcentage de la mesure de l'exposition totale)		
EU 14a	Exigences de fonds propres supplémentaires pour faire face au risque de levier excessif (%)		
EU 14b	dont : à satisfaire avec des fonds propres CET1 (points de pourcentage)		
EU 14c	Exigence de ratio de levier SREP totales (%)	3,00 %	3,00 %
	Exigence de coussin lié au ratio de levier et exigence de ratio de levier globale (en pourcentage de la mesure de l'exposition totale)		
EU 14d	Exigence de coussin lié au ratio de levier (%)		
EU 14e	Exigence de ratio de levier globale (%)	3,00 %	3,00 %
		a	E
		31/12/2022	**31/12/2021**
	Ratio de couverture des besoins de liquidité		
15	Actifs liquides de qualité élevée (HQLA) totaux (valeur pondérée -moyenne)	3 786 265	5 435 104
EU 16a	Sorties de trésorerie — Valeur pondérée totale	530 818	935 807
EU 16b	Entrées de trésorerie — Valeur pondérée totale	1 408 662	1 994 530
16	Sorties de trésorerie nettes totales (valeur ajustée)	132 704	233 952
17	Ratio de couverture des besoins de liquidité (%)	595,77 %	388,53%
	Ration de financement stable net		
18	Financement stable disponible total	17 067 889	19 258 501
19	Financement stable requis total	10 646 793	12 107 880
20	Ratio NSFR (%)	160,31%	159,06%

02

CATÉGORIES DE RISQUE

2.1 | Risque de crédit - Informations qualitatives générales sur le risque de crédit (EU CRA)

2.1.1 Définition du risque de crédit

Le risque de crédit : risque de pertes résultant de l'incapacité des clients de la banque, d'émetteurs ou d'autres contreparties à faire face à leurs engagements financiers. Le risque de crédit inclut le risque lié aux activités éventuelles de titrisation et peut être aggravé par le risque de concentration individuelle, pays ou sectorielle.

Dispositif de sélection des opérations

ECM ne gère qu'un seul produit dénommé Plan d'Epargne Crédit des Militaires, qui comportait deux phases essentielles, une phase d'épargne suivie d'une phase de prêt. Depuis 2013 ce contrat n'est plus commercialisé mais les contrats en cours, en phase d'épargne et en phase de crédit, poursuivent leurs effets jusqu'à leur terme.

2.1.1.1. Phase d'épargne

Lors de la souscription à ce plan d'épargne, un gestionnaire d'ECM s'assurait que le bulletin de souscription était dûment renseigné par le souscripteur et que les documents justificatifs obligatoires étaient bien tous fournis. Il utilisait ces informations afin de contrôler l'exhaustivité et la cohérence des informations par rapport au contrat proposé. Il vérifiait également que la durée de contrat était comprise entre 5 et 15 ans et que l'âge du souscripteur était compatible avec la durée de l'épargne et du prêt.

2.1.1.2. Phase de crédit

Le risque de crédit demeure limité par la mise en place de ratios stricts pour l'octroi des prêts. En outre, une sûreté sur le crédit accordé est systématiquement requise ainsi qu'une assurance emprunteurs.
Les demandes de crédit sont instruites par les gestionnaires ECM, puis contrôlées et validées par le Directeur Général délégué avant d'être signées par le Directeur général.
Pour chaque demande de crédit, le gestionnaire rédige une fiche de synthèse reprenant le descriptif de l'opération et l'étude de faisabilité afférente (revenus et justificatifs, charges, apport personnel et composition, taux d'endettement…).

Lorsque le dossier est complet et que le taux d'endettement n'excède pas 40 %, le gestionnaire procède à la rédaction de l'offre de prêt et de la lettre d'accompagnement.

Un suivi spécifique est mis en place depuis le 1er janvier 2022 pour les prêts dont le ratio d'endettement dépasse 35%, conformément aux décisions du HCSF. En cas de critères non-conformes aux critères habituels, le Directeur Général délégué sollicite un comité de crédit avec le Directeur général. La décision finale est du ressort du Directeur général.

Les critères d'octroi de crédit ECM sont définis dans le manuel de procédures ECM. Les gestionnaires n'ont aucune délégation pour dépasser ces critères.

Par ailleurs, ECM a constitué dans ses comptes un fonds mutuel de garantie des emprunteurs alimenté par la prime d'épargne (Fonds A) ainsi que par les intérêts produits par cette prime (Fonds B). Ce fonds a pour objet de couvrir les créances irrécouvrables constatées au titre des prêts consentis par la société ECM. En 2022, aucun contentieux n'a été constaté sur les prêts ECM en cours.

Dispositif de sélection des émetteurs d'obligation

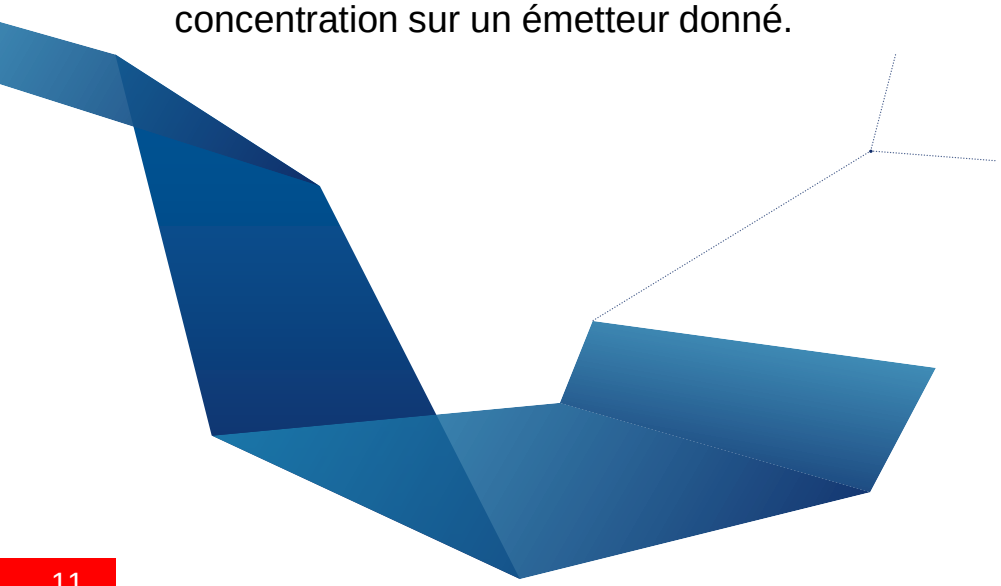
Les émetteurs d'obligation appartenant à la catégorie "investisseur" font l'objet d'une sélection, encadrée par une méthodologie spécifique.

En premier lieu, une fiche de synthèse crédit sur la base de la recherche crédit externe à disposition est établie, elle comprend le profil de l'émetteur, des analyses SWOT et concurrentielles ainsi qu'une comparaison sectorielle de certains indicateurs (solvabilité, rentabilité, taille, etc.). Des limites sectorielles et structurelles ont été définies pour atteindre une forte diversité. Un seuil minimal de liquidité des souches obligataires est également requis.

Tout nouvel émetteur doit être validé par le comité des placements et par la suite intégré à la liste des obligataires autorisés.

Tout au long de la vie de l'obligation (laquelle ayant vocation à être détenue jusqu'au terme) des suivis de la situation et de la notation de l'émetteur sont mis en place, avec recours éventuel au comité des risques, pour décider d'une cession lorsque le risque est réputé intenable pour ECM.

Des limites d'exposition sont suivies pour atténuer le risque de concentration sur un émetteur donné.



Mesure et surveillance du risque de crédit

Au cours de la phase d'épargne, le cumul des versements programmés et exceptionnels pour tous les contrats d'épargne d'une même cellule familiale ne peut excéder 16 000 € sur une période de douze mois consécutifs. L'accord préalable de la société ECM est requis en cas de dépassement éventuel.

Il résulte de ce montant de versement annuel plafonné des montants prêtés également limités, les droits à prêt étant directement associés à l'épargne accumulée.

Depuis janvier 2022, les informations relatives au suivi du risque de crédit à l'octroi sont fournies trimestriellement au Conseil d'administration de la société ECM, afin de suivre le respect des critères énoncés par le HCSF.

Tenant compte des éléments décrits ci-dessus (auxquels s'ajoutent les cautions et sûretés mises en place), le risque de crédit pour ECM peut être évalué supportable.

Dispositif en cas de créances impayées

Les cas d'échéances de prêts impayées sont, dans les faits, extrêmement rares au cours de la vie d'un crédit pour les clients ECM.

Néanmoins, le process en place prévoit qu'en cas d'insuffisance de provisions, les créances impayées soient remontées via un reporting à la Direction Générale.

Stress tests

Des stress scenarii sont réalisés à minima annuellement afin de vérifier l'adéquation des fonds propres par rapport aux risques de crédit dans un contexte d'activité dégradée.

L'établissement simule 4 scenarii différents :

- Conditions de marché défavorables affectant la valeur du produit net bancaire ;
- Utilisation complète des droits à prêts par les bénéficiaires de contrats, préjudiciable à ECM, qui constate en moyenne 20% des droits non utilisés ;
- Une hausse des frais généraux ;
- Le défaut d'un ou plusieurs émetteurs au sein du portefeuille d'actifs.

Dans l'ensemble de ces scénarii, ECM disposerait de leviers managériaux lui permettant de satisfaire aux exigences réglementaires.

Vérification et réexamen du dispositif de gestion du risque de crédit

Le dispositif de gestion des risques (organisation, indicateurs, limites, suivi) fait l'objet d'une validation par le Comité Exécutif et le Comité des risques du Groupe AGPM. Le comité des risques est informé des résultats des contrôles et travaux réalisés sur ce dispositif.

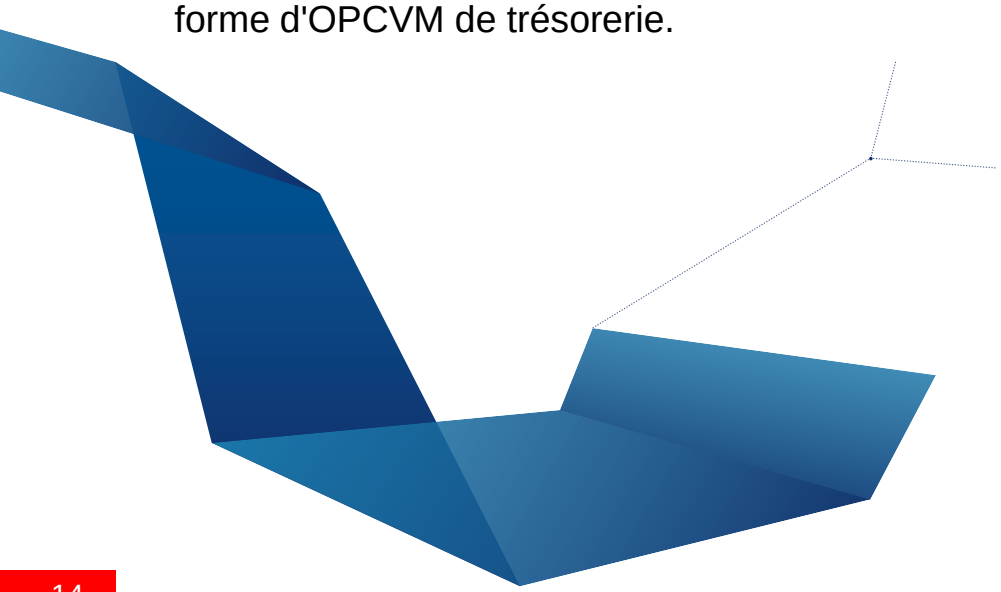
Le risque de concentration

ECM a défini une limite par contrepartie plus conservatrice que la limite réglementaire. Ainsi, la société ECM ne peut être engagée sur une même contrepartie ou un même groupe de contreparties pour plus de 10% des fonds propres.

Concernant les expositions sur les établissements de crédits (ou les groupes d'établissements), ECM applique une limite équivalente à 100% de ses fonds propres.

2.2 | Risque de marché - Exigences de publication d'informations qualitatives sur le risque de marché (EU MRA)

La Banque n'a pas vocation à supporter un risque direct de marché significatif. Elle ne dispose pas d'un portefeuille à vocation spéculative. Les seules positions pour compte propre autorisées sont enregistrées en portefeuille de placement sous forme d'OPCVM de trésorerie.



2.3 | Risque opérationnel - Informations qualitatives sur le risque opérationnel (EU ORA)

Définition du risque opérationnel

Les risques opérationnels : risque de pertes résultant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes d'information ou d'événements extérieurs.

Cette catégorie de risque comprend notamment :

- **Les risques de non-conformité :** risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, du fait de l'absence de respect des dispositions législatives et réglementaires, des normes et usages professionnels et déontologiques, propres aux activités des banques ;

- **Le risque de réputation :** risque résultant d'une perception négative de la part des clients, des contreparties, des actionnaires, des investisseurs ou des régulateurs, pouvant affecter défavorablement la capacité de la Banque à maintenir ou à engager des relations d'affaires et la continuité d'accès aux sources de financement ;

- **Le risque de conduite inappropriée :** risque résultant d'action (ou inactions), de comportements de la Banque ou de ses employés pouvant aboutir à des conséquences négatives pour les parties prenantes, ou mettant en risque la pérennité ou la réputation de la Banque ;

- **Les risques IT et de sécurité des systèmes d'information** (cybercriminalité, défaillance de services…).

Identification et mesure du risque opérationnel

De par ses activités, ECM peut être exposée aux risques humains, organisationnels, logistiques, relationnels, de sécurité, de fraude, de non-conformité, risques liés au système d'information.

Le dispositif mis en place dans ECM pour maîtriser le risque opérationnel s'inscrit dans celui mis en place par le Groupe AGPM de manière proportionnée aux risques portés par la société.

Les exigences de fonds propres pour le risque opérationnel sont déterminées via la méthode élémentaire.

Les dispositifs mis en place

2.3.3.1 Maîtrise du risque opérationnel

Le dispositif décrit ci-après est celui en place au sein du Groupe AGPM qu'ECM applique proportionnellement aux risques qu'elle porte.

Ce dispositif s'articule autour du contrôle interne. Une organisation de l'activité est mise en place en portant une attention à la séparation des tâches. Des documents sont à la disposition du personnel pour la bonne exécution des tâches leur incombant. Ces documents sont révisables tous les trois ans sauf nécessité immédiate.

Au sein du Groupe AGPM, des objectifs sont fixés en termes de traitement d'appels, de dossiers, de réclamations. Des plans d'actions spécifiques sont ensuite mis en place afin de tendre vers la réalisation de ces objectifs.

Pour aider à la maîtrise du risque opérationnel, des moyens sont alloués aux entités du Groupe AGPM, notamment humains, financiers, matériels mais aussi en matière de système d'information et de pilotage afin de suivre au plus près les indicateurs pertinents.

Ce dispositif intègre notamment trois dispositifs particuliers :

- Un plan de continuité d'activité destiné à assurer la gestion des crises et situations pouvant mettre l'entreprise en difficulté;
- Un plan préventif de rétablissement visant à renforcer les dispositifs de gestion de crise ;
- Un dispositif de fiabilisation et de protection des données des entités AGPM, des clients et des salariés impliquant à la fois les directions productrices ou gestionnaires de données.

Ce dispositif comporte également un système de pilotage, notamment au regard de l'actualisation des cartographies mais également du suivi des résultats de contrôle ou des incidents, ainsi qu'un système de reporting pour les différents comités.

2.3.3.2 Contrôle du risque opérationnel

Une note d'organisation générale rédigée par la Direction Générale précise l'organisation mise en place pour servir la stratégie et les principes généraux de fonctionnement du Groupe AGPM.

Dans ECM, deux services gèrent les activités principales de la société comme les crédits et investissements (front et back office). Un service est également chargé des travaux comptables et de l'établissement des reportings d'ECM.

Ces services sont placés sous la responsabilité de responsables de services hiérarchiquement rattachés au Directeur Général Délégué qui est également Directeur financier et technique des entités du Groupe AGPM.

Une répartition claire des tâches a été faite entre responsable de service et gestionnaire de contrat, et fait l'objet d'une documentation.

Des dispositions peuvent être prises pour assurer la sécurité des collaborateurs via des actions de sensibilisation et la dispense de formations. Des protocoles et procédures ont également été développés afin d'assurer la sécurité des personnes.

Des dispositions ont aussi été prises pour assurer la sécurité des locaux et des équipements. Un dispositif renforcé a été mis en place pour assurer la sécurité des infrastructures informatiques.

Enfin, des mesures et actions sont déployées pour protéger les informations à caractère confidentiel, comprenant notamment une sensibilisation du personnel aux règles en vigueur.

2.3.3.3 Procédures et modes opératoires

Pour limiter le risque opérationnel, des procédures sont développées pour les différentes activités qu'exerce ECM, mais également en matière de gestion comptable et réglementaire, de lutte contre le blanchiment d'argent et le financement du terrorisme. Des modes opératoires spécifiques aux métiers ont été établis.

Ces procédures et modes opératoires constituent une documentation détaillée permettant aux collaborateurs d'effectuer au mieux leurs tâches tout en atténuant le risque opérationnel auquel la société ECM est exposée.

2.3.3.4 Pilotage du risque opérationnel

Le dispositif de pilotage des entités du groupe sur lequel s'appuie ECM s'articule autour de ressources humaines et de moyens matériels et technologiques.

Au niveau humain, ce pilotage comporte plusieurs axes, au premier rang desquels l'évaluation des collaborateurs qui permet de mesurer l'adéquation des ressources aux objectifs fixés. Elle permet également d'apprécier le comportement professionnel du collaborateur au regard de sa fonction et de fixer ses objectifs pour l'année à venir. Une attention particulière est portée à la formation, et notamment au maintien et à l'acquisition des compétences professionnelles afin de permettre une gestion efficace des activités. La DRH prend toutes les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des collaborateurs. Au niveau matériel et technologique, la mise à jour des logiciels et l'implémentation de nouvelles technologies permettent aux collaborateurs d'effectuer au mieux leurs tâches et d'assurer une gestion, un suivi et un contrôle plus efficients.

Plan de continuité d'activité

2.3.4.1 Principales caractéristiques

L'entité ECM s'appuie sur le dispositif de résilience du Groupe AGPM qui vise à garantir le maintien en action des processus majeurs.

Il comporte quatre volets :

- Une politique de résilience ;
- Un plan de reprise informatique (PRI) ;
- Un plan de continuité des activités métier (PCA) ;
- Un plan de gestion de crise (PGC).

Ce dispositif de résilience a vocation à couvrir tous les scénarii ayant un impact significatif sur la continuité des activités critiques. Sont dès lors pris en considération tous les événements impactant les opérations et les missions critiques, les collaborateurs, les systèmes d'information ou encore la réputation de l'ensemble des entités AGPM. Plusieurs scénarii ont donc été étudiés.

Les activités métiers sont priorisées en fonction des impacts que provoquerait leur arrêt. Il est ainsi attribué, à chaque processus métier, un objectif de délai de reprise dérivé de la sévérité de l'impact de son arrêt éventuel.

2.3.4.2 Vérification de l'efficacité du dispositif

Le plan de secours informatique est testé annuellement. Les contrôles permanents de premier niveau sur ce domaine sont du ressort de la Direction des systèmes d'information.

La continuité de l'alimentation électrique est quant à elle testée régulièrement du fait de l'utilisation de groupes électrogènes les jours où le tarif de l'électricité est au plus haut.

Un compte rendu des tests réalisés, comportant leurs objectifs, un bilan de synthèse, les points de non-conformité et le cas échéant un plan d'actions correctives, est transmis annuellement à la Direction générale, au Directeur des systèmes d'information ainsi qu'à la fonction gestion des risques.

Le plan de continuité des activités ainsi que le plan de gestion de crise doivent être testés annuellement.

2.3.4.3 Formalisation et actualisation du dispositif

Le dispositif de résilience est formalisé. Une mise à jour annuelle du plan est prévue.

Elle comprend un inventaire et une évaluation des procédures existantes, permettant de gérer la continuité des métiers et d'assurer la reprise en cas d'arrêt des activités.

2.3.4.4 Mise en œuvre du plan de continuité

Le plan de reprise informatique (PRI) n'a pas été activé en 2022.
La cellule de gestion de crise a été sollicitée régulièrement pour assurer un suivi du risque sanitaire. La tenue d'une cellule de crise spécifique à la pandémie a été subordonnée au suivi d'indicateurs épidémiologiques au sein du Groupe AGPM et dans son environnement.

Gestion du risque informatique

La gestion du risque informatique est une activité itérative ayant notamment vocation à définir la stratégie de maîtrise des risques, identifier les domaines à risque, les évolutions du niveau de risque afin de pouvoir prendre des décisions de priorisation ou de réorientation des mesures de sécurité.

Le RSSI (Responsable de la Sécurité des Systèmes d'Information) anime le dispositif de gestion des risques informatiques. Pour ce faire, il s'appuie sur une équipe de référents DSI (Direction des Systèmes d'Information) représentant tous les métiers de l'informatique (Pilotage, Produits Développements, Opérations, Sécurité, Support).

L'outil de base de la gestion de ces risques est la cartographie des risques informatiques. Ce document est mis à jour dans le cadre d'ateliers trimestriels et une synthèse est publiée annuellement.

En 2022, les résultats de cette cartographie ont été présentés aux administrateurs dans le cadre du comité des risques.

2.3.5.1 Le dispositif de contrôle permanent

Le dispositif de contrôle du système d'information est identique et intégré à celui du Groupe AGPM.

Les contrôles sont organisés en 3 niveaux :

- Les contrôles de premier niveau sont intégrés aux outils ou réalisés au sein de la Direction des systèmes d'information ;

- Les contrôles de deuxième niveau incombent au service contrôle interne et au RSSI, tous deux rattachés au Secrétariat général ;

- Les contrôles de troisième niveau sont du ressort du service audit interne qui est rattaché à la Direction générale.

2.3.5.2 Cartographie des risques

Une cartographie est établie et permet de déterminer la criticité de chaque catégorie de risque informatique, il en ressort que pour ECM ce sont les risques cyber qui représentent les plus forts risques opérationnels.

Sécurité du système d'information

2.3.6.1 Politique de sécurité

Cette politique traite, entre autres, des problématiques de gestion des risques intégrant les risques cyber et leur rapide évolution afin de maintenir les risques au niveau de tolérance défini ainsi que des mesures de sécurité à mettre en œuvre, sur la base de l'évaluation des risques. Elle définit la gouvernance de la sécurité du système d'information. Elle concerne également la protection des données, la gestion des accès et des nouveaux usages, les modalités de définition, maintien, amélioration, mise à l'épreuve de la résilience, la continuité d'activé ainsi que le respect des règlementations en vigueur en matière de sécurité de l'information.

2.3.6.2 Organisation

La Direction générale décide de l'organisation de la gestion de la sécurité de l'information, de la stratégie de sécurité et des objectifs à atteindre.

Elle a désigné un responsable de la sécurité des systèmes d'information qui est rattaché au Secrétariat Général afin de garantir l'indépendance et l'objectivité de la fonction sécurité vis-à-vis de la Direction des systèmes d'information qui regroupe les fonctions informatiques.

Le RSSI intervient en qualité d'expert métier sur les questions de sécurité des systèmes d'information.

2.3.6.3 Gestion des incidents

Les incidents sont enregistrés et documentés en mentionnant les faits, leurs effets et les mesures prises pour y remédier. Le cas échéant, il est précisé s'il s'agit d'une violation de données à caractère personnel. Cette documentation doit permettre de réévaluer l'impact d'un incident lorsque de nouveaux éléments sont communiqués ultérieurement.

Un processus définit les modalités de notification des divulgations ou des accès non autorisés aux données, aux autorités (CNIL, DRSD) et prévoit l'information sans délai des personnes concernées par la divulgation ou l'accès non autorisé à leurs données.

Les éléments techniques relatifs aux incidents sont conservés pendant une durée d'au moins 6 mois et de maximum un an. Un plan de réponse aux incidents cybers majeurs est en cours de préparation. Celui-ci sera destiné à gérer l'incident et limiter les dommages opérationnels. Ce plan doit définir l'organisation (interne et externe) ainsi que les étapes à suivre afin de revenir à un état stable.

Sur 2022, avec l'aide d'un prestataire, les outils et l'organisation permettant de répondre à un incident impactant les serveurs et les postes de travail ont été mis en place.

2.3.6.4 Programme de sensibilisation

Les collaborateurs sont des acteurs de la sécurité au quotidien, dans tous les gestes ou actions conduits au niveau du SI. Dès lors, un programme de formation à la sécurité de l'information est établi pour l'ensemble des collaborateurs afin de s'assurer qu'ils sont sensibilisés régulièrement au risque de sécurité informatique par des campagnes de e-learning, des tests de phishing ainsi que des messages circonstanciés notamment au risque cyber et en capacité de réagir.

Détection et gestion des incidents

2.3.7.1 Les incidents opérationnels

Le processus de contrôle est réalisé par le biais d'un contrôle de la bonne exécution sur l'ordonnanceur. En cas d'erreur de traitement ou de problème, un message d'alerte est envoyé automatiquement à l'exploitation.

En cas d'incident et selon la possibilité, soit le processus de reprise est mis en œuvre, soit un ticket est envoyé au support de niveau 2 pour l'analyse et la résolution de l'incident.

2.3.7.2 Les incidents de sécurité

En 2022, avec l'aide d'un prestataire, un centre opérationnel de Sécurité SOC* externalisé a été mis en place. Celui-ci est chargé de surveiller 24h/24 et 7j/7 les événements de sécurité impactant les serveurs et les postes de travail.

** Centre opérationnel de sécurité (SOC) : emplacement centralisé où une équipe de sécurité supervise, détecte, analyse et prend en charge les incidents de cyber-sécurité, généralement 24h/24*

Le SOC exploite des outils lui permettant de détecter les attaques au plus près des acteurs du SI (postes de travail et serveurs). Il détecte tous changements de comportements et, à l'aide d'intelligence artificielle, reste efficient en limitant les faux-positifs.

La politique de réponse à une attaque est stricte : isoler dès la détection la machine incriminée qui constitue la source de l'alerte avant que l'attaque ne puisse se déployer.

Selon les études, ce type de service couvre 60% à 80% des risques cyber. Les risques d'attaques sur des composants d'infrastructures seuls ne sont pas détectés. En 2022, le dispositif a été complété par un SIEM intégrant notamment d'autres sources d'événements et permettant l'analyse et la corrélation d'événements afin compléter les outils de détection.

Pour la réponse aux incidents de sécurité, le dispositif sera complété en 2023 par un autre service externalisé chez un prestataire de réponse aux incidents de sécurité ou PRIS, à même de porter assistance en cas d'attaque.

03

GOUVERNANCE ET GESTION DES RISQUES

3.1 | Approche de l’établissement en matière de gestion des risques (EU OVA)

Structure de la gestion des risques

La gestion des risques d'ECM s'articule autour de plusieurs acteurs.

- Le Conseil d’administration, en tant qu’organe de contrôle, est responsable de la gestion des risques. Il approuve les politiques réglementairement contraignantes et leurs mises à jour. Il s’assure également de leur application. Il contrôle la mise en œuvre, par les dirigeants effectifs, des dispositifs de surveillance afin de garantir une gestion efficace et prudente de la société. Il approuve également les rapports réglementaires.

- **Le comité d’audit** émet un avis sur les politiques d’audit interne et de contrôle interne, approuve le plan d’audit annuel. Il examine les résultats des missions de l’audit interne et s’assure du suivi des recommandations y afférentes.

- **Le comité des risques** émet un avis sur les politiques de risques, de contrôle interne, de conformité, la cartographie des risques et examine les rapports réglementaires. Il s’assure de l’efficacité du dispositif de maîtrise des risques.

- **Les dirigeants effectifs,** représentant l'organe exécutif en charge de la mise en œuvre opérationnelle des orientations validées par le Conseil, proposent la politique de gestion des risques. Ils sont membres permanents du comité technique des risques et coordonnent in fine la résolution des incidents opérationnels en cas d’escalade.

Au sein du Groupe AGPM, un comité technique des risques a été mis en place afin de surveiller les expositions aux risques des entités AGPM mais également de réaliser les suivis des dispositifs mis en place, et notamment les dispositifs de maîtrise des risques et de la solvabilité. Il est également en charge de coordonner et de diffuser la culture du risque.

Promotion de la culture du risque

Le Groupe AGPM a développé une culture du risque, qui, pour être efficace, nécessite l'engagement des organes de gouvernance.

Le Conseil d'administration et la Direction générale s'impliquent en tant que promoteurs et superviseurs de la culture du risque : les principes de bonne gestion des risques sont présentés aux collaborateurs. Ceux-ci bénéficient de formations, soit au travers du rappel des règles, lors de la déclaration d'un incident ou de la mise à jour de la cartographie des risques, soit au travers d'e-learning relatifs au dispositif de sécurité du système d'information, notamment. La volonté des organes de gouvernance est de promouvoir la culture des risques, afin que les collaborateurs intègrent les notions de risque et de sa gestion dans leurs activités au quotidien et puissent ainsi adapter leurs comportements.

Identification des risques

3.1.3.1 La cartographie des risques

L'identification et l'évaluation des risques reposent sur deux approches distinctes.

Pour les risques opérationnels, outre l'approche « Top Down » menée par l'équipe gestion des risques, une approche « Bottom Up » réalisée, à partir des processus/activités de l'entreprise, sur la base d'ateliers regroupant, notamment, le service contrôle interne et les équipes opérationnelles.

Concernant les autres risques majeurs, une approche à la fois descendante (Top Down) et montante (Bottom Up) est menée par l'équipe gestion des risques, sur la base d'entretiens avec les administrateurs (notamment pour les risques stratégiques et émergents), dirigeants, directeurs, fonctions clés, responsables opérationnels les plus pertinents.

Les risques identifiés sont rattachés aux processus concernés, classifiés selon une typologie de référence, décrits avec précision afin d'en faciliter l'analyse ultérieure.
Dans les deux cas, les risques sont évalués selon une grille de fréquence et de sévérité et priorisés au moyen d'une matrice de criticité.

La cartographie des risques majeurs du Groupe AGPM, incluant ECM, est présentée au moins annuellement au comité des risques et au Conseil d'administration.

3.1.2.2 Plans d'actions sur les risques identifiés dans la cartographie

L'exploitation des résultats de contrôles, des incidents, les revues de risques, de Dispositif de Maitrise des Risques (DMR) permettent d'établir des plans de remédiation, en concertation avec les interlocuteurs concernés au sein des directions.

Ces actions, définies au regard des risques identifiés, peuvent poursuivre l'objectif de réduire, transférer, éviter, accepter les risques. Elles font l'objet d'un suivi particulier.

Déclaration des risques et des incidents significatifs

La fonction gestion des risques établit trimestriellement un reporting général des risques destiné au Président, aux dirigeants, et aux membres du comité des risques.

Suite à la dérogation obtenue auprès de l'ACPR, le plan préventif de rétablissement est présenté bisannuellement au Conseil.
Le Directeur Général Délégué présente en outre trimestriellement les ratios prudentiels au Conseil d'administration.

La fonction gestion des risques établit trimestriellement un reporting des risques au niveau du Groupe, destiné entre autres au comité des risques, contenant une restitution sur les principaux incidents du trimestre. Elle alerte la Direction générale en cas d'incident significatif.

Aucun incident significatif n'a été détecté dans le cadre de l'application des procédures.

En cas de difficultés économiques nécessitant d'activer le plan préventif de rétablissement, la Direction générale d'ECM en informe le Conseil d'Administration à qui incombe la validation de la mise en œuvre du plan.

Déclaration sur les risques

Le Conseil d'administration d'ECM a formellement approuvé lors de sa séance de juin 2022 son appétence au risque, adaptée aux enjeux extinctifs d'ECM.

Cette appétence introduit des seuils prudentiels minimaux, la nécessité absolue de maintenir des fonds propres positifs tout au long de l'extinction du portefeuille, y compris en cas de stress, et des règles de maintien de liquidité minimale avant d'envisager des investissements de long terme.

ECM dispose d'une politique de gestion des risques qui a été mise à jour et validée lors du conseil d'Administration qui s'est tenu le 6 décembre 2022.

Surveillance et suivi des risques

Une veille est effectuée pour les risques émergents. Pour les risques déjà identifiés dans la cartographie, une revue périodique est réalisée. Certains évènements ayant un impact majeur, l'émergence de nouveaux risques ou des rapports d'audit relevant des dysfonctionnements peuvent amener à la réalisation d'une revue de la cartographie.

Gestion des risques

3.1.7.1 Dotation en fonds propres

Afin de pallier ses différents risques, ECM a été dotée, dès sa création, d'un capital important permettant de couvrir une partie des frais généraux par le placement desdits fonds propres.

L'UES (Union d'Economie Sociale) ECM étant détenue intégralement par deux entités (AGPM Assurances et AGPM Vie, sociétés d'assurance mutuelles), sa solvabilité repose sur la capacité financière de ses associés. Dans un contexte d'arrêt de production depuis le 1er janvier 2013, les simulations effectuées visent à vérifier que, dans les scénarii centraux et dans des scénarii stressés, les fonds propres permettent de respecter les ratios prudentiels, d'assurer une capacité à détenir des liquidités suffisantes et restent positifs jusqu'à l'extinction du portefeuille.

Le rachat des parts de l'association Tégo a été effectué courant 2022 : AGPM Vie détient à présent 8/15 de la société, le solde étant détenu par AGPM Assurances.

A l'issue de cette opération, un pacte a été signé entre les deux sociétés et ECM pour assurer un soutien en fonds propres et en liquidité.

3.1.7.2 Référentiel de gestion des risques

Le dispositif de gestion des risques est encadré principalement par la politique de gestion des risques du Groupe AGPM qui définit l'objet, les objectifs, le périmètre, la gouvernance et la mise en œuvre de la politique, la comitologie et la gouvernance des risques, le reporting et la surveillance risques, les rôles et responsabilités de chacun dans le dispositif.

3.1.7.3 Prise de risque

L'établissement ECM étant géré de manière extinctive et sa taille diminuant régulièrement, la stratégie mise en œuvre consiste à réduire les risques au minimum de façon à assurer les engagements jusqu'à l'extinction des contrats.

Différents dispositifs ont été mis en œuvre à cette fin, notamment :

- Ne pas accepter de risque de marché autre que sur des OPCVM monétaires ;

- Détenir les obligations à leur terme, sauf risque de crédit majeur ;

- Maintenir un haut niveau de liquidités et ne pas considérer de nouveaux investissements de long terme si les scenarii de stress exhibent une potentielle insuffisance de trésorerie à horizon 2 ans ;

- Assurer la diversification sectorielle et géographique des émetteurs obligataires, avec en particulier un système de limites ;

- Limiter le risque lié à l'octroi de prêts, ceux-ci étant par nature limités en montant, sur la base de critères de sélection de prêts et la mise en place d'un double regard entre le Directeur général et le Directeur général délégué.

Le contrôle interne

Le dispositif de contrôle interne des entités du Groupe AGPM visant à permettre d'assurer la maîtrise des risques comporte 3 niveaux.

Le niveau 1 consiste en la maîtrise des activités au jour le jour. Les pratiques les plus efficaces de gestion des risques sont mises en place au niveau de chaque processus. Ce premier niveau consiste également en la réalisation de contrôles intégrés aux outils de gestion ou mis en œuvre directement par les opérationnels. Une communication d'informations appropriées est faite à la deuxième ligne de défense.

Le niveau 2 consiste en la structuration et la coordination du dispositif de maîtrise des activités. Il permet d'apporter une assistance aux opérationnels dans l'identification et l'évaluation des principaux risques des entités AGPM et du dispositif de maîtrise des risques en place, dans la rédaction de politiques, de procédures, la conception de contrôles pertinents. Il s'assure du bon fonctionnement et l'efficacité du dispositif en place.

Le niveau 3 est une évaluation globale et indépendante du dispositif. La fonction d'audit interne, indépendante, fournit à travers une approche fondée sur les risques, une assurance globale sur l'organisation et l'efficacité des 2 premiers niveaux de maîtrise, aux instances de surveillance et à la Direction générale.

3.1.8.1 Le contrôle permanent

Le contrôle permanent relève :

- Pour les contrôles de niveau 1, des directions métiers,

- Pour les contrôles de niveau 2, de services dédiés dont le service contrôle interne, le service conformité, le DPO et le RSSI, qui peuvent également avoir des missions relatives au périmètre ECM.

Le Service contrôle interne est rattaché au Secrétariat général et n'exerce aucune activité opérationnelle. Il assiste la Direction générale, dans la mise en place, l'optimisation et le pilotage du dispositif de contrôle interne, appliqué au risque opérationnel.

Il existe également un service conformité qui, comme le service contrôle interne, est hiérarchiquement rattaché au Secrétariat général et n'exerce aucune autre fonction au sein du Groupe.

3.1.8.2 Le comité des risques

Il a pour mission d'émettre un avis sur :

- Les politiques mises en œuvre en matière de gestion des risques, de contrôle interne, de conformité et de s'assurer de leur mise en œuvre,

- La cartographie des risques et veiller à son actualisation régulière,

- Le dispositif de maîtrise des risques,

- Les rapports réglementaires établis.

Il s'assure également de l'efficacité du dispositif de gestion des risques.

Ce comité des risques créé au sein du Conseil d'administration d'AGPM Groupe suit le dispositif de maîtrise des risques et en rend compte au Conseil d'administration. Il soumet à approbation les éventuelles mesures à prendre afin de tendre vers une meilleure maîtrise des risques encourus.

Il peut effectuer des études sur des risques nécessitant une attention particulière pouvant lui être présentés afin qu'il en tienne le Conseil d'administration informé. Il examine en outre l'ensemble des rapports statutaires et donne son avis lors du vote au Conseil d'administration.

3.1.8.3 La fonction de gestion des risques

La fonction gestion des risques est rattachée au Secrétariat général et n'exerce aucune autre fonction au sein du Groupe.

Elle a pour mission essentielle d'animer l'ensemble des dispositifs d'identification, de mesure, de traitement, de surveillance des risques, pour toutes les entités AGPM.

Son action se fonde notamment sur une politique de gestion des risques.

3.1.8.4 Le contrôle périodique

Il a pour rôle de s'assurer de l'efficience du dispositif de contrôle interne. Il est placé sous la responsabilité de la fonction d'audit interne, rattachée à la Direction générale.

L'action de l'audit se fonde sur une politique d'audit interne, soumise à la validation du Conseil d'administration, qui explicite le rôle, la méthodologie de l'audit interne, le dispositif de pilotage de l'activité, ainsi que les droits et obligations de l'auditeur et de l'audité. Elle a fait l'objet d'une actualisation en 2022. Elle repose également sur un plan d'audit pluriannuel, validé annuellement par le Conseil d'administration.

Les missions d'audit donnent lieu à la formulation de recommandations qui sont présentées aux directions concernées. Les actions validées par le management sont attribuées à un pilote et soumises à un délai de réalisation.

Les rapports d'audit sont transmis aux administrateurs, membres du comité d'audit.

04

FONDS PROPRES ET EXIGENCES DE FONDS PROPRES

4.1 | Vue d'ensemble des montants totaux d'exposition au risque (EU OV1)

		Montant total d'exposition au risque (TREA)		Exigences totales de fonds propres
		a	b	c
		31/12/2022	31/12/2021	31/12/2022
1	Risque de crédit (hors CCR)	12 135 104	13 003 672	970 808
2	Dont approche standard	12 135 104	13 003 672	970 808
3	Dont approche NI simple (F-IRB)			
4	Dont approche par référencement			
EU 4a	Dont actions selon la méthode de pondération simple			
5	Dont approche NI avancée (A-IRB)			
6	Risque de crédit de contrepartie - CCR			
7	Dont approche standard			
8	Dont méthode du modèle interne (IMM)			
EU 8a	Dont expositions sur une CCP			
EU 8b	Dont ajustement de l'évaluation de crédit - CVA			

9	Dont autres CCR			
10	Sans objet			
11	Sans objet			
12	Sans objet			
13	Sans objet			
14	Sans objet			
15	Risque de règlement			
16	Expositions de titrisation dans le portefeuille hors négociation (après le plafond)			
17	Dont approche SEC-IRBA			
18	Dont SEC-ERBA (y compris IAA)			
19	Dont approche SEC-SA			
EU 19a	Dont 1 250 % / déduction			
20	Risques de position, de change et de matières premières (Risque de marché)			
21	Dont approche standard			
22	Dont approche fondée sur les modèles internes			
EU 22a	Grands risques			

23	Risque opérationnel	270 946	277 100	21 676
EU 23a	Dont approche élémentaire	270 946	277 100	21 676
EU 23b	Dont approche standard			
EU 23c	Dont approche par mesure avancée			
24	Montants inférieurs aux seuils de déduction (soumis à pondération de 250 %)			
25	Sans objet			
26	Sans objet			
27	Sans objet			
28	Sans objet			
29	**Total**	**12 406 049**	**13 280 773**	**992 484**

05

TABLE DE CORRESPONDANCE

Article CRR	Concordance	Tableau
435 1a	Partie 2.1 - Risque de crédit - Informations qualitatives générales sur le risque de crédit (EU CRA)	CRA
	Partie 2.2 - Risque de marché - Exigences de publication d'informations qualitatives sur le risque de marché (EU MRA)	MRA
	Partie 2.3.3 - Les dispositifs mis en place Partie 2.3.4 - Plan de continuité d'activité Partie 2.3.6.3 - Gestion des incidents Partie 2.3.7 - Détection et gestion des incidents	ORA
	Partie 3.1.6 - Gestion des risques Partie 3.1.2.2 - Plans d'actions sur les risques identifiés dans la cartographie	OVA
435 1e	Partie 3.1.4 - Déclaration sur les risques	OVA
435 1f	Partie 3.1.4 - Déclaration sur les risques	OVA CRA
438 d	Partie 4.2 - Vue d'ensemble des montants totaux d'exposition au risque (EU OV1)	OV1
447	Partie 1 - Les indicateurs clés (EU KM1)	KM1
450	Comme indiqué dans l'introduction ECM, les états liés aux rémunérations ne sont pas applicables dans la mesure où l'établissement ne dispose d'aucun effectif salarié et que les mandataires sociaux ne sont pas rémunérés par ECM	

Groupe AGPM

SANTÉ · PRÉVOYANCE · ASSURANCE · RETRAITE