Memo Bank

Résilience numérique et continuité d'activité

1. Comment lire ce document

La sécurité, la disponibilité et la résilience de nos services constituent le fondement de la confiance que vous nous accordez. En tant qu'établissement de crédit dédié aux entreprises, Memo Bank a fait le choix d'une architecture technologique et d'une gouvernance des risques sans compromis, pleinement alignée sur les exigences prudentielles applicables aux établissements de crédit, notamment celles du règlement (UE) n°2022/2554 dit DORA (Digital Operational Resilience Act) et celles de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque.

Cette note synthétise les mesures mises en œuvre par Memo Bank pour assurer sa résilience opérationnelle. Pour des informations plus complètes sur le dispositif de gestion des risques de l'établissement, le rapport de « Pilier 3 » est annexé au rapport annuel publié sur notre site web. Nous vous invitons aussi à consulter nos Conditions générales d'utilisation et notre Politique de protection des données personnelles.

2. Principes fondamentaux de l'architecture technique : résilience par conception

L'infrastructure informatique de Memo Bank est conçue selon des principes techniques stricts visant une résilience intrinsèque et une diminution radicale du risque humain.

A. Architecture *Cloud-agnostic* et Multi-Régions

***Infrastructure-as-a-Service* (IaaS) :** Memo Bank ne recourt qu'à des fournisseurs de cloud de premier plan basés dans l'Union Européenne : Google Cloud Platform (GCP) et Amazon Web Services (AWS).

***Cloud-agnostic* et Multi-Prestataires :** Memo Bank privilégie une approche *cloud-agnostic*. La migration complète de l'environnement de production d'AWS vers GCP, en juin 2025, a démontré la faisabilité technique d'un basculement total de prestataire. AWS reste mobilisable comme fournisseur de repli.

Résilience géographique : l'infrastructure est déployée selon une architecture multi-régions (France et Belgique), fonctionnant en mode actif/passif pour permettre une bascule rapide entre régions. Chaque région est subdivisée en trois zones physiques indépendantes.

B. Sécurité et Immutabilité des Systèmes

Infrastructure immutable : notre infrastructure est par nature « immutable », ce qui signifie qu'elle n'est pas modifiable en cours d'utilisation. Sa gestion est assurée par un processus de déploiement continu entièrement automatisé, minimisant le risque d'erreur humaine et d'altération malveillante des systèmes en production.

Architecture sans mot de passe : l'accès au Core Banking System (CBS) repose exclusivement sur des certificats éphémères et individuels. L'authentification est renforcée par des mécanismes d'authentification forte (2FA) et d'authentification unique (SSO) y compris pour les accès aux applications SaaS.

Accès Sécurisé : l'accès aux applications est strictement contrôlé via un **double Réseau Virtuel Privé (VPN)** et des clés de **chiffrement**.

3. Gouvernance, contrôle et gestion des risques

Notre dispositif de gestion des risques repose sur une gouvernance claire et un contrôle permanent rigoureux, englobant les risques opérationnels et les risques d'externalisation.

A. Contrôle interne

Le **Conseil de Surveillance**, avec l'éclairage du **Comité d'audit et des risques** (dont Memo Bank s'est volontairement dotée alors que sa taille de bilan ne justifierait pas la constitution obligatoire d'un tel comité spécialisé) définit et révise le Cadre d'Appétit aux Risques, qui inclut des indicateurs spécifiques au risque opérationnel lié aux technologies d'information et de communication.

Ce cadre est mis en œuvre par les **dirigeants effectifs**, et la **Direction des Risques, du Contrôle interne et de la Conformité (DRCC)**, qui veillent à la cohérence et l'efficacité du dispositif global de contrôle interne.

Un **Responsable de la Sécurité des Systèmes d'Information (RSSI)** rattaché au pôle Risques de la DRCC, apporte une appréciation indépendante des risques vis-à-vis de la Direction Technique.

B. Maîtrise du risque d'externalisation

Politique KYS : le dispositif *Know Your Supplier* (KYS) assure la maîtrise des risques liés aux tiers externes, y compris les Prestataires de Services Essentiels Externalisés (PSEE), incluant une analyse préalable des risques opérationnels avant tout nouveau contrat soutenant une fonction critique.

Conformité des contrats de prestation au règlement DORA : une démarche proactive a été menée pour adapter les contrats des fournisseurs TIC soutenant des fonctions critiques, afin d'assurer leur conformité à l'article 30 du règlement DORA. Cela protège notamment Memo Bank contre les cas de résiliation unilatérale par le prestataire, en garantissant des périodes de maintien de services et

ménageant des stratégies de sortie — par exemple, 1 an de préavis pour un prestataire critique comme GCP ou Enfuce (processeur de paiements par cartes bancaires).

4. Continuité d'activité et tests de résilience

A. Planification et Scénarios de Crise

Pour établir le **Plan d'Urgence et de Poursuite d'Activité**, Memo Bank conduit une analyse d'incidence sur les processus critiques ou importants de l'établissement. Il s'agit de prévoir notamment les scénarios suivants :

- Défaillance d'une région chez un fournisseur cloud (supposant donc au préalable la défaillance cumulée des trois sites dans la même région) ;
- Rupture de la relation contractuelle avec un fournisseur cloud ;
- Incidents majeurs impactant les TIC ou les paiements.

Memo Bank ne dispose **pas d'actifs informatiques physiques** autres que des postes entièrement banalisés, dont le contenu est chiffré, et qui n'accèdent aux applications du Core Banking System qu'à travers un réseau privé virtuel. Il n'existe donc aucun risque physique pouvant mettre en péril la continuité d'activité.

B. Tests de Résilience Opérationnelle Numérique

Exercices réguliers : Memo Bank conduit **au moins deux fois par an** des *Disaster Recovery Tests* simulant une bascule d'une région active du fournisseur cloud vers une autre région (France → Belgique, Belgique → France). Ces tests, conduits dans l'environnement de pré-production, démontrent la capacité à rétablir l'ensemble des services en quelques heures après la coupure initiale.

Objectif de Perte de Données (RPO) : les exercices de crise démontrent aussi la capacité de Memo Bank à ne **pas perdre plus d'une minute de données**.

Gestion des Incidents : les obligations de notification aux autorités compétentes (ACPR pour les incidents majeurs TIC/Paiement sous **4 heures** et CNIL pour les violations de données personnelles sous **72 heures**) sont strictement respectées. Depuis son lancement en 2020, Memo Bank n'a jamais constaté aucun incident opérationnel ou de paiement majeur ou significatif (au sens de la directive DSP2 ou du règlement DORA). Le taux de disponibilité (*uptime*) a atteint **99.9996 %** sur l'exercice 2024.

Audits externes : en plus du programme d'audit (contrôle périodique) que tout établissement de crédit est tenu de mettre en place, Memo Bank mandate régulièrement des sociétés de cybersécurité de premier plan pour des tests de pénétrations et des audits de sécurité sur l'infrastructure (par exemple lors de la migration en production d'AWS vers GCP en juin 2025).

Convention de niveau service (SLA) : si les conditions particulières qui vous lient à Memo Bank le prévoient, vous pouvez bénéficier d'un SLA notamment en matière de disponibilité de l'API Premium, de réactivité du support clients, et d'indemnisation (voir l'Annexe F des CGU).