Directive n° 47/G/2007 du 31 août 2007 relative au plan de continuité de l'activité au sein des établissements de crédit

Le Gouverneur de Bank Al-Maghrib ;

vu la loi n° 34-03 relative aux établissements de crédit et organismes assimilés promulguée par le dahir n° 1-05-178 du 15 moharrem 1427 (14 février 2006), notamment son article 51 ;

vu les dispositions de la circulaire n° 40/G/ 2007 du 2 août 2007 relative au contrôle interne des établissements de crédit ;

après examen par le Comité des établissements de crédit lors de sa réunion tenue en date du 23 juillet 2007 ;

fixe par la présente directive les règles minimales devant être observées par les établissements de crédit pour la mise en place d'un plan de continuité de l'activité.

Objet de la Directive

La présente directive s'inscrit dans le cadre de la mise en œuvre du deuxième pilier de Bâle II. Elle constitue un référentiel de saines pratiques pour la mise en place par les établissements de crédit, désignés ci-après par « établissement», du plan de continuité de l'activité.

I- Définitions

Au titre de la présente Directive on entend par :

Plan de continuité de l'activité (PCA) : un plan d'action écrit qui expose les procédures et détermine les processus et les systèmes nécessaires pour poursuivre ou rétablir les opérations d'une organisation en cas de perturbation opérationnelle.

Perturbation opérationnelle majeure : une perturbation à fort impact sur les opérations normales des activités, affectant une grande zone urbaine ou géographique et les communautés voisines qui lui sont économiquement intégrées. Outre la menace sur les opérations normales des établissements, les perturbations opérationnelles majeures affectent les infrastructures physiques.

Les perturbations opérationnelles majeures peuvent résulter d'un grand éventail d'événements, comme des catastrophes naturelles, des attaques terroristes et d'autres actes intentionnels ou accidentels qui causent des dégâts s'étendant aux infrastructures physiques. D'autres événements, comme les pannes informatiques, les virus technologiques et les pandémies peuvent conduire à des perturbations opérationnelles majeures en affectant le fonctionnement normal des infrastructures physiques.

Les événements extrêmes qui peuvent avoir un impact significatif sont ceux qui causent habituellement la destruction de l'infrastructure physique et des équipements

ou des dégâts sévères, la perte ou l'indisponibilité de personnel et la restriction d'accès à la zone affectée.

Opération ou service critique : Toute activité, fonction, processus ou service, dont la perte aurait des conséquences substantielles sur la continuité des opérations de l'établissement et/ou du système financier. Les exemples de services critiques pour un système financier incluent notamment, le traitement des paiements de montants importants, la compensation et le règlement des transactions et le support aux systèmes comme les services de réconciliation et de financement.

Analyse d'impact sur l'activité : Le processus qui consiste à mesurer (quantitativement et qualitativement) l'impact sur l'activité ou les pertes dans les processus métiers en cas de perturbation opérationnelle. Elle est utilisée pour identifier les priorités, les ressources et le personnel nécessaires pour la reprise de l'activité ainsi que pour aider à formuler un plan de continuité de l'activité.

II- Politique et responsabilités en matière de plan de continuité de l'activité.

A) Rôle de l'organe d'administration

Il incombe à l'organe d'administration (conseil d'administration, conseil de surveillance ou toute autre instance équivalente) d'approuver la stratégie, la politique et les objectifs de continuité de l'activité de l'établissement. Il doit être tenu régulièrement informé de l'état de la continuité.

La stratégie de continuité de l'activité porte notamment sur les points suivants :
- la sensibilisation de tout le personnel quant à l'importance de la continuité de l'activité et du plan de continuité ;
- l'identification des fonctions, processus et systèmes critiques de l'établissement qui doivent prioritairement être repris en cas de perturbation opérationnelle majeure ;
- la détermination de la durée maximale acceptable par l'établissement pour restaurer les fonctions, processus et systèmes critiques après une interruption due à une perturbation opérationnelle majeure ;
- la détermination du niveau de reprise jugé acceptable des services fournis et le délai admis pour la reprise de l'activité normale après une interruption due à une perturbation opérationnelle majeure ;
- la distribution des rôles et la définition des responsabilités et des lignes de reporting en matière de continuité de l'activité ;
- l'application des mesures préventives pour réduire les risques liés aux perturbations opérationnelles majeures ;
- l'affectation du budget et des moyens nécessaires au plan de continuité de l'activité.

B) Rôle de l'organe de Direction

L'organe de direction (direction générale, directoire, ou toute autre instance équivalente) met en œuvre la stratégie de continuité de l'activité, telle qu'approuvée par l'organe d'administration, et établit le plan de continuité de l'activité de l'établissement. A cet effet, il :

- désigne un responsable du plan de continuité de l'activité, chargé de développer, de mette à jour et de tester ce plan;
- met en place un comité de crise et un groupe de gestion de la continuité de l'activité ;
- définit les principaux rôles, responsabilités et pouvoirs (incluant des substituts) en matière de continuité de l'activité ;
- crée et promeut une culture qui affecte un degré élevé de priorité à la continuité d'activité ;
- établit, au moins une fois par an, un rapport sur le plan de continuité de l'activité qu'il adresse à l'organe d'administration.

III- Scénarios de crise et analyses d'impact

L'établissement procède des analyses d'impact préalablement à la mise en place d'un plan de continuité de l'activité.

Ces analyses doivent permettre d'évaluer les niveaux de risque liés aux perturbations opérationnelles et les différents scénarios applicables à ces situations.

Selon le niveau de risque évalué, l'établissement :
- identifie les fonctions, processus et systèmes critiques qui doivent être prioritairement repris en cas de perturbation opérationnelle majeure ;
- définit ses objectifs de reprise d'activité (les niveaux et délais de reprise attendus) ;
- alloue les ressources humaines et matérielles nécessaires.

L'analyse d'impact tient compte des principaux paramètres suivants :
- l'emplacement des installations critiques de l'établissement et leur sensibilité aux événements de risque majeurs ;
- les facteurs géographiques (par exemple, la concentration des établissements dans les zones d'activité de grandes villes) ;
- la nature et la complexité des activités de l'établissement ;
- la taille et l'extension géographique du réseau de l'établissement ;
- le degré de centralisation/décentralisation des fonctions essentielles ou processus critiques ou de leur externalisation :
- les contraintes résultant de divers types de dépendance, y compris celles vis-à-vis des fournisseurs, de clients, et d'autres établissements.

L'analyse d'impact couvre également les interactions avec les risques encourus par l'établissement notamment les risques de crédit, de marché, opérationnels et de liquidité.

IV- Composantes du plan de continuité de l'activité

Le plan de continuité de l'activité comprend les mesures, procédures et informations, nécessaires pour appréhender et gérer les conséquences d'une interruption due à une perturbation opérationnelle majeure. Les principales composantes de ce plan sont les suivantes :
- les stratégies et les procédures de protection et de récupération des données (électroniques ou matérielles) ;

- les procédures de secours pour les données, les applications et le matériel importants ;
- les sites alternatifs de remplacement (centres de secours) prédésignés situés à une distance prudente des locaux principaux ;
- les ressources minimales pour le rétablissement des fonctions ou des processus essentiels ;
- les processus pour la restauration ou le remplacement des informations importantes (sous forme électronique et sur papier) ;
- les niveaux et les délais de reprises attendus ;
- la validation des capacités de reprise de l'activité de ses fournisseurs de services essentiels (en cas d'activités externalisées) ;
- les conditions dans lesquelles un état d'urgence doit être déclenché.

V- Ressources humaines

L'établissement identifie les ressources humaines critiques et définit les modalités selon lesquelles ces ressources peuvent être amenées à fonctionner aux différents endroits convenus (bureaux, équipements et approvisionnements,…). Le recours à des collaborateurs intérimaires ou à des spécialistes externes peut également être envisagé.

Il prend les mesures nécessaires pour s'assurer que l'ensemble du personnel est informé du contenu du plan de continuité de l'activité et des différentes révisions qui y sont apportées.

Le plan de continuité de l'activité doit faire partie des programmes de formation de l'établissement.

VI- Tests et modifications du plan de continuité de l'activité

L'efficacité des mesures de continuité de l'activité (en particulier celles relatives aux centres de secours à distance) est évaluée au moyen de tests dont la fréquence, la profondeur et le détail sont en fonction de l'importance des risques liés aux éléments testés.

Les fonctions, les processus et les systèmes critiques doivent être testés en intégrant les risques liés aux clients, les sous-traitants et les contreparties bancaires importantes ainsi que la défaillance des infrastructures financières. Les résultats de ces tests sont documentés, analysés et communiqués à l'organe d'administration et de direction, à l'audit interne et aux différentes entités concernées. Ils servent à la modification, le cas échéant, du plan initial et d'autres aspects de la gestion de continuité d'activité de l'établissement.

Dans certains cas, les modifications peuvent résulter de changements dans les activités, les responsabilités, les systèmes, les logiciels, les matériels, le personnel, ou les équipements ou l'environnement externe.

VII- Communication interne et externe

Le plan de continuité de l'activité de l'établissement incorpore des protocoles et procédures de communication d'urgence. Ces procédures doivent notamment :
- identifier le groupe de personnes responsable de communiquer avec le personnel et les divers partenaires externes. Ce groupe devrait être capable de communiquer avec le personnel localisé dans des sites isolés, répartis sur plusieurs emplacements ou éloignés du siège.Il pourrait inclure l'organe de direction, la fonction communication, la fonction juridique, la fonction conformité ainsi que le personnel responsable des procédures de continuité d'activité de l'établissement ;
- définir le processus de communication interne ;
- se baser sur tout protocole de communication qui existe déjà dans le système financier et inclure des listes de contacts avec les autorités de supervision et les autres établissements pour faciliter une évaluation de la situation du système financier et coordonner les efforts de reprise de l'activité. Les contacts avec les services de secours là où les ressources critiques sont localisées doivent être identifiés et consignés ;
- traiter des questions connexes qui peuvent surgir pendant une perturbation opérationnelle majeure, comme la disponibilité de moyens multiples de communication (ex : des téléphones fixes digitaux et analogiques, des téléphones portables, des téléphones satellitaires, la messagerie de texte, des sites Web, des dispositifs à main sans fil, etc.) en faveur du personnel clef de l'établissement ;
- prendre en compte le fait qu'une perturbation des opérations puisse affecter significativement les opérations d'une filiale ou succursale dans le pays d'accueil. Dans ce cas, des protocoles de communication doivent être établis par l'établissement pour traiter les circonstances dans lesquelles il faudrait entrer en contact avec les autorités de supervision du pays d'accueil.

VIII- La continuité des activités externalisées

L'externalisation des activités critiques (notamment les systèmes d'informations, les centres de secours…) implique le maintien de relations régulières avec le prestataire du service et l'application des mêmes exigences, en matière de continuité aux activités externalisées.

L'établissement prend toutes les démarches raisonnables pour s'assurer que les services externalisés seront disponibles en cas de nécessité, par exemple en veillant à une distance géographique suffisante entre les centres de secours et les centres opérationnels, ou en intégrant dans la convention de sous-traitance des garanties de capacité.

IX- Audit interne

L'audit interne de l'établissement doit réaliser des vérifications périodiques du plan de continuité de l'activité et de l'approche globale de la gestion de la continuité. Il est également appelé à participer aux séances d'essai de l'établissement et, le cas échéant, à celles des prestataires de service qui prennent en charge les activités critiques externalisées et à en évaluer les résultats.

X- Reporting destinés à Bank Al-Maghrib

Les établissements communiquent à Bank Al-Maghrib le rapport sur le plan de continuité de l'activité qu'ils adressent à l'organe d'administration.