Foire aux questions
sur le nouveau guide de remplissage
de l'annexe sur les moyens de paiement

Cette FAQ concerne exclusivement l'annexe sur la sécurité des moyens de paiement du rapport prévue par l'article 43 du règlement CRBF n° 97-02. Elle constitue une synthèse des réponses aux questions soulevées par certains établissements concernant le guide de remplissage et la grille d'auto-évaluation, actualisés en 2011. Elle sera régulièrement mise à jour.

Questions sur le périmètre de l'annexe

Lors des précédents exercices, nous devions fournir des statistiques de volumétrie et de fraude pour chaque moyen de paiement. Ceci est-il toujours d'actualité ?

Réponse BDF

Non. À compter de l'exercice 2012 (sur les données 2011), plus aucune de ces données n'est demandée. Les données en volume sont en effet transmises dans le cadre de la cartographie sur les moyens de paiement, et les données de fraude sont déclarées *via* le questionnaire *ad hoc*. On notera en particulier le transfert des données de fraude sur les transactions par carte dans le questionnaire fraude, lequel devra faire l'objet d'une adaptation afin de les intégrer.

Questions sur la partie identification des moyens de paiement

- ***Il est demandé « d'identifier les moyens de paiement émis ou gérés par l'établissement » : en matière de clientèle, pouvez-vous préciser s'il s'agit bien de décrire la clientèle utilisatrice du moyen de paiement ou la clientèle cible du moyen de paiement et confirmer que vous n'attendez pas la répartition du moyen de paiement par segment de clientèle (en nombre et valeurs) ?***

  Réponse BDF

  Une simple description de la clientèle cible est attendue à travers cette question. À compter de l'exercice 2012 aucune donnée volumétrique ne sera demandée dans cette annexe, il n'est donc pas attendu du déclarant de présenter une segmentation de sa clientèle.

- ***Qu'entend-on par « modalités de fonctionnement » ? Doit-on détailler les différentes versions du moyen de paiement (par exemple : les cartes de débit, de crédit, de débit-crédit…) ?***

Réponse BDF
Concernant les moyens de paiement classiques (cartes de crédit, de débit…), il est attendu de nommer simplement le moyen de paiement sans décrire son fonctionnement ; si le moyen de paiement est innovant (par exemple : paiement mobile, paiement électronique, prépayé, sans contact, etc.), il conviendra d'expliquer brièvement comment fonctionne ce moyen de paiement.

- ***Pouvez-vous définir la notion de cartes privatives (non CB ? cartes de retrait propriétaires ?) dans les mêmes termes que ceux employés pour la cartographie des moyens de paiement ?***

Réponse BDF
Les cartes privatives sont des cartes de paiement dont les opérations d'émission et d'acquisition sont gérées par la même entité (au sein de systèmes « à trois coins »). Les cartes de retrait propriétaires, conformément à la cartographie des moyens de paiement, ne sont pas considérées comme des cartes privatives.

- ***Tableau des différents cas : dans le cas où le tableau personnalisé GCB est non complété par l'établissement, pourquoi ne demande-t-on pas de remplir le tableau joint relatif aux autres cartes non CB ?***

Réponse BDF
Le tableau GCB est un modèle de reporting complet pour les cartes interbancaires « CB ». Si ce dernier n'est pas complété par l'établissement, le tableau joint peut tout à fait être utilisé. Inversement, l'établissement peut utiliser le modèle GCB pour ses autres catégories de cartes s'il en a convenance.

Questions sur la partie « procédures et mesures pour maîtriser les risques »

- ***Dans l'identification des risques, s'agit-il de décrire simplement le risque ou de compléter cette description par la « probabilité qu'un événement ou une situation se produise » (fréquence), son « impact avant la prise en compte des mesures de prévention ou des mesures correctives » ?***

Réponse BDF
Il est attendu de l'établissement une description du risque, avec appréciation de son impact potentiel et la probabilité de survenance de ce risque.

- ***« Évaluer la probabilité » : est-ce la probabilité de survenance annuelle ?***

Réponse BDF
Oui, il s'agit bien de la probabilité de survenance annuelle.

- ***« Son impact avant prise en compte des mesures » : comment qualifier l'impact ? doit-on simplement le décrire, ou le quantifier (et particulièrement le chiffrer en montant) ?***

Réponse BDF
Il peut sembler délicat d'évaluer l'impact sans le mesurer. Si des éléments factuels permettant de mesurer le niveau de risque brut peuvent être apportés, il conviendra de les reporter ici.

- ***En résumé sur ces points, s'agit-il bien d'insérer dans ce cadre les éléments de la cartographie des risques ? Si oui, jusqu'à quel niveau de détail ?***

  Réponse BDF
  Oui, en se limitant aux moyens de paiement. Le niveau d'extraction à retenir dépend de l'organisation de l'établissement et de la profondeur de son analyse de risques, sachant qu'il est proposé de répondre sous forme de tableau (donc avec un niveau de granularité à apprécier en conséquence).

- ***« Décrire de manière succincte les risques subsistants » : donc une simple description du risque résiduel est-elle suffisante ?***

  Réponse BDF
  Oui. Si ce risque résiduel est mesurable, indiquer le montant de son impact.

Questions sur la partie « contrôles axés sur les moyens de paiement »

- ***Jusqu'à quel niveau de détail des contrôles « métier » doit-on rentrer ?***

  Réponse BDF
  Il est attendu des établissements une description sommaire des contrôles permanents de niveau 1 et 2. Il est à noter que les contrôles de premier niveau (effectués par les opérationnels) peuvent être considérés comme des mesures de couverture. Les autres contrôles (effectués par le service conformité par exemple) sont à décrire dans la partie « contrôles axés sur les moyens de paiement ».

- ***L'objet du contrôle doit décrire « à quel niveau du processus a été effectué ce contrôle » ; cela implique-t-il la description de tous les processus liés aux moyens de paiement ?***

  Réponse BDF
  Non, sous réserve que la description donnée permette de comprendre à quelle tâche il est fait référence.

- ***Les résultats négatifs des contrôles doivent-ils donner lieu systématiquement à des plans d'actions de correction ou des actions correctives (le risque zéro n'existant pas…) ?***

  Réponse BDF
  Dans le cas où les contrôles identifient des zones de risques avec un plan d'action à mettre en œuvre, alors oui, celui-ci doit être mis en œuvre. L'établissement peut toutefois accepter la présence d'un risque résiduel dûment justifié.

- ***En résumé sur ces points, s'agit-il bien de décrire les résultats des contrôles permanents de premier niveau (et de second niveau ?) sur la sécurité des moyens de paiement ?***

  Réponse BDF
  En résumé sur ces points, il s'agit non seulement de décrire les contrôles *permanents* de premier et second niveaux, mais aussi l'ensemble des contrôles *périodiques* axés sur les moyens de paiement. On attend ici de l'établissement une description de l'organisation de ces contrôles, du niveau de rattachement des personnes chargées de les effectuer, des résultats de ces contrôles, des plans d'actions mis en œuvre pour pallier les éventuels dysfonctionnements constatés et enfin des plans de suivi qui en découlent.

Questions sur la grille d'analyse

- ***Que veut dire « méthodologie reconnue » ? Doit-on citer le nom de l'outil de gestion des risques opérationnels ? Pouvez-vous donner des exemples ?***

  Réponse BDF
  Pour ce qui est des méthodologies reconnues, il est fait référence à l'une des méthodes communément admises pour la gestion des risques opérationnels. (Exemples : ISO/IEC 27005, qui donne les lignes directrices pour gérer les risques en sécurité de l'information ; EBIOS, qui est une méthode d'appréciation et de traitement des risques sur les systèmes d'informations ; MEHARI qui est une méthode d'analyse et de management des risques ; ou encore OCTAVE, qui est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels…). Si une telle méthodologie est utilisée par l'établissement, il convient de la citer. Dans le cas où ce dernier utilise une méthodologie interne, on pourra en donner les grandes lignes directrices.

- ***Qu'entend-on par « priorité » dans le critère d'évaluation du système d'identification des risques « les risques identifiés sont classés par ordre de priorité » ?***

  Réponse BDF
  On entend par là le niveau du risque selon les critères de classification de votre établissement (par exemple : faible/moyen/fort, de 1 à 5, etc.).

- ***Que veut dire le critère « l'analyse des risques donne lieu à des actions spécifiques, dont la responsabilité est clairement définie » ? Est-ce à dire que la cartographie des risques doit être régulièrement actualisée ? contrôlée ? que les plans d'actions et les actions correctives doivent être régulièrement suivis ?***

  Réponse BDF
  Il s'agit d'identifier qui est responsable de la mise en œuvre des plans d'actions et de s'assurer que chaque risque identifié donne bien lieu à un plan d'action, sauf si le risque est accepté par l'établissement. Les plans d'actions et les actions correctives doivent également être validés et régulièrement suivis.

- ***Par « porteurs de risque », entend-on bien « entités portant le risque au plan financier » plutôt qu'« opérationnel » ?***

  Réponse BDF
  Les deux sont fréquemment confondus, mais cela dépend de l'organisation interne. On entend ici les personnes/services affectés par le risque brut (les principaux concernés, impactés, que ce soit au niveau opérationnel ou financier).

- ***Sur la « périodicité des contrôles », que veut dire « couvrir le périmètre dans un délai raisonnable » ?***

  Réponse BDF
  Le contrôle périodique doit couvrir l'ensemble du périmètre auditable dans un délai qui dépend de chaque établissement, de ses moyens alloués aux contrôles, de son appréciation des risques, etc. Indiquer ce délai et pourquoi il a été fixé à ce niveau (à titre d'exemple, le fait que l'ensemble du périmètre ne soit couvert qu'en 15 ans peut soulever des questions…).

- ***La notion de « degré de maîtrise » (dans le paragraphe mesure de couverture) correspond-elle bien à l'efficacité du dispositif de maîtrise ? Doit-on l'exprimer en pourcentage ou la qualifier globalement (faible, moyenne, forte) ?***

  Réponse BDF
  Il s'agit d'apprécier (d'« auto-évaluer ») votre degré de maîtrise du risque brut et de ses incidences. Êtes-vous bien en mesure de mesurer l'impact, la probabilité de survenance, etc., relatifs à un risque donné ? Le choix de l'indicateur appartient à chaque banque selon sa méthode.

- ***Que veut dire « participent au choix des mesures » ? Sont-ils décideurs, coauteurs, simplement informés…***

  Réponse BDF
  « Participent » sous-entend d'être actifs dans le processus et ne pas seulement être informés.

- ***Qu'appelle-t-on, pour le critère (c) (dans la partie impact des mesures de couverture et de suivi des risques) une « veille » ? Pouvez-vous donner des exemples ?***

  Réponse BDF
  La veille consiste à se tenir au courant des nouveaux risques apparaissant sur le marché (nouveau risque informatique, nouveau type de fraude, etc.).

- ***Pour le critère (c) (partie périodicité des contrôles), qu'est-ce que des « indicateurs précis pour définir la fréquence des contrôles » ? Pouvez-vous donner des exemples ?***

  Réponse BDF
  Il s'agit d'indiquer sur quelle base est définie la fréquence minimale d'audit pour un service/département donné.