RÉFÉRENTIEL DE SÉCURITÉ DU CHÈQUE

NOTICE DE REMPLISSAGE DU QUESTIONNAIRE D'ÉVALUATION DE LA SÉCURITÉ DU CHÈQUE

MARS 2023

AVANT PROPOS

L'autoévaluation annuelle par les établissements bancaires de la sécurité des processus de traitement du chèque vise à assurer la sécurité de ce moyen de paiement et, *in fine*, à maintenir la confiance des utilisateurs dans ce moyen de paiement. Cet exercice s'appuie sur un référentiel de sécurité établi par la Banque de France en concertation avec les établissements assujettis dans le cadre du Comité Français d'Organisation et de Normalisation Bancaires (CFONB), et que l'IEOM a fait le choix d'étendre aux établissements financiers des Collectivités françaises du Pacifique.

Face à l'augmentation sensible de la fraude au chèque en Métropole à partir de 2016 tant en volume qu'en montant malgré la baisse observée des transactions, l'Observatoire de la sécurité des moyens de paiement scripturaux (OSMP) a mené en 2020 et 2021 une étude spécifique pour mieux connaître les phénomènes de fraude au chèque en identifiant les principales vulnérabilités de ce moyen de paiement et en émettant des recommandations pour lutter contre le développement de la fraude. Dans ce cadre, l'Observatoire a exprimé 10 recommandations publiées dans son rapport annuel 2020[1], qui s'adressent à l'ensemble des acteurs intervenant sur le cycle de vie du chèque, des utilisateurs aux professionnels de la filière du chèque, en premier lieu les établissements bancaires et leurs prestataires. Ces recommandations sont également applicables dans les Collectivités françaises du Pacifique

La nouvelle version du RSC intègre explicitement les 10 recommandations de l'OSMP et précise certaines exigences.

À travers ce nouveau référentiel de sécurité, l'IEOM appelle notamment les établissements financiers à :

- **Renforcer la surveillance des remises frauduleuses de chèque, notamment au regard des risques d'escroqueries sur les encaissements de chèque ;**
- **Améliorer la lutte contre les chèques perdus et volés, en renforçant la sécurité de l'acheminement des chéquiers, la qualité des procédures de mises en opposition et la diffusion d'outils de contrôle de la régularité des chèques ;**
- **Maintenir la vigilance sur la sécurité physique des formules, en précisant les attentes sur les éléments de sécurité qui doivent limiter les risques de falsification et de contrefaçon.**

Au final, le nouveau RSC et le questionnaire d'évaluation associé contiennent 9 objectifs de sécurité, auxquels sont associés 26 considérations-clés et 116 critères d'appréciation (soit 1 considération-clé et 16 critères d'appréciation supplémentaires par rapport à la version précédente).

La table de correspondance entre les différentes versions du RSC est fournie au § 5.2 de la présente notice.

En outre, des modifications sont également apportées sur les trois points suivants :

1) un commentaire sur l'évaluation est dorénavant requis pour chaque situation de type « Ne Nous Concerne Pas » (NNCP), pour chaque considération-clé pour laquelle l'évaluation ne conclut pas à une pleine conformité (notation 1, 2 ou 3), et enfin pour chaque considération-clé pour laquelle l'évaluation a évolué d'une année sur l'autre à la hausse comme à la baisse (y compris lorsque la notation est montée à 4).

2) la qualification d'incident grave est explicitée et harmonisée pour l'ensemble de la Place au travers de critères communs, ce qui a un impact sur l'appréciation de toutes les considérations-clés (cf. l'annexe « *IEOM RSC Annexe Identification notification des incidents graves chèque*s »).

3) l'appréciation de l'augmentation significative de la fraude, c'est-à-dire l'évolution défavorable et importante au cours de l'exercice évalué des cas ou des montants de fraude au chèque par rapport à l'exercice précédent, qui peut par exemple être comprise comme une hausse supérieure à 10%, est également définie et harmonisée pour l'ensemble des déclarants.

Un fichier Excel, « IEOM RSC Objectifs sécurité & Considérations clés » est joint à la présente notice. En amont du dépôt de la déclaration RSC sous ONEGATE, il reprend la démarche de notation des Considérations clés et permet de préparer les réponses du questionnaire. En outre, il restitue une mesure du nombre de caractères renseignés dans le commentaire associé à la notation de chaque Considération Clé.

[1] Observatoire de la sécurité des moyens de paiement, Rapport annuel 2020, juillet 2021 : chapitre 4 « *Étude sur la fraude au chèque : enseignements et recommandations* »

TABLE DES MATIERES

1. OBJET DU DOCUMENT

La présente notice à l'usage des déclarants est **exclusivement destinée aux établissements qui sont assujettis à la déclaration annuelle auprès de l'Institut d'Emission d'Outre-Mer (IEOM) du rapport « Référentiel de sécurité du chèque » (« RSC »), sous ONEGATE-OSCAMPS.**

Elle a pour objet de faciliter :

- la compréhension globale du référentiel de la sécurité du chèque ;
- l'évaluation aux critères d'appréciation posés dans le questionnaire associé.

Elle est destinée aux établissements pour la bonne compréhension du RSC et aux remettants qui auront la responsabilité de compléter le formulaire en mode saisie dit « U2A » (*User to Application*) sur le portail ONEGATE.

Pour bien appréhender le vocabulaire, l'utilisation des zones de réponse, la méthode d'évaluation et le remplissage du document, il est indispensable de prendre connaissance du **Référentiel de sécurité du chèque** (RSC) et du **Questionnaire d'évaluation de la Sécurité du Chèque** avant d'examiner la présente notice à l'usage des déclarants. Ces documents seront prochainement accessibles sur le site de l'IEOM.

Le RSC, fourni par l'IEOM, exprime les objectifs de sécurité se rapportant au chèque. Le renseignement du questionnaire d'évaluation de la sécurité du chèque par le déclarant constitue la déclaration annuelle sur le respect du RSC sous la forme d'un rapport annuel d'autoévaluation.

Le référentiel de sécurité du chèque constitue une base d'autoévaluation des mesures de couverture des risques inhérents au Système de paiement par chèque dont les établissements doivent tenir compte pour améliorer leurs politiques de gestion des risques. Les résultats d'auto-évaluation au RSC doivent refléter la politique de maitrise des risques de chaque établissement ainsi que les éventuels points d'attention ou les actions correctrices à mettre en œuvre. Il s'agit de promouvoir une efficience des processus des établissements au regard de la sécurité globale du système de paiement par chèque.

Dans le cadre de sa mission de surveillance, l'IEOM vérifie le respect des objectifs de sécurité à travers l'analyse des notations découlant de l'exercice d'autoévaluation du déclarant et des commentaires associés. Selon le résultat de l'évaluation, l'IEOM peut être amené à solliciter des informations complémentaires, voire à poursuivre ses investigations par des évaluations sur pièces ou sur place. Il peut également être conduit à formuler des recommandations à l'établissement concerné.

2. LE RAPPORT ANNUEL D'AUTOÉVALUATION DE LA SÉCURITÉ DU CHÈQUE

2.1. Finalités du rapport annuel d'autoévaluation

Le rapport d'autoévaluation de la sécurité du chèque est l'outil de reporting annuel qui permet à l'IEOM d'assurer sa mission de surveillance de la sécurité du moyen de paiement « chèque » ;

Les résultats de l'exercice d'évaluation sont déclarés à l'IEOM, afin de mesurer dans le temps l'évolution des risques sur le système de paiement par chèque.

Pour les établissements assujettis, l'exercice d'évaluation au RSC constitue un instrument d'autodiscipline. Le RSC doit servir de référence pour leurs fonctions de contrôle interne ainsi que pour leurs relations avec l'ensemble des acteurs de la filière.

En revanche, l'exercice d'évaluation au RSC n'a pas vocation à remonter à l'IEOM une information sur l'offre de produits et de services liés au chèque, sur l'organisation opérationnelle de l'activité ou sur l'évolution de la fraude au cours de l'année et les dispositifs de maîtrise des risques mis en place. **À partir de 2023, les établissements doivent en conséquence remplir la partie consacrée au chèque de l'annexe du rapport annuel sur le contrôle interne, à l'instar des autres moyens de paiement,** tel qu'exigé à l'article 262 de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (ACPR).

Les établissements demeurent responsables des prestations qu'ils ont pu déléguer ou faire sous-traiter. Ainsi, pour l'ensemble de la filière et des objectifs de sécurité généraux et spécifiques, le terme « établissement » doit être compris comme « établissement et prestataire » lorsque les fonctions considérées sont réalisées par un sous-traitant.

2.2. Périmètre des établissements assujettis à la collecte

Les établissements soumis à la déclaration annuelle du rapport RSC sont les établissements financiers agissant en qualité d'établissement assujetti tiré de chèque ou en qualité d'établissement assujetti présentateur, ainsi que le Trésor public, la Banque de France, les offices des postes et télécommunication, l'institut d'émission d'outre-mer et la Caisse des dépôts et consignations.

Chaque année, l'IEOM définit la liste des établissements assujettis à la collecte des autoévaluations au RSC sur la base des informations contenues dans le Registre des agents financiers (REGAFI) tenu par l'Autorité de contrôle prudentiel et de résolution et des activités de chèque déclarées par les établissements dans la collecte de l'IEOM « *Cartographie des moyens de paiement scripturaux* ». L'IEOM adresse un courriel de lancement aux établissements assujettis, qui peut être adapté pour les nouveaux établissements assujettis. Elle ouvre les obligations déclaratives dans ONEGATE par domaine. Pour le chèque, il s'agit du Rapport « Respect du référentiel du chèque », code du domaine « OSI ».

2.3. Les opérations concernées

Les opérations couvertes par le rapport d'autoévaluation sont détaillées dans le RSC au chapitre 2 « Périmètre ». Il s'agit notamment de l'ensemble des opérations par chèque, dès lors que l'établissement déclarant est tiré ou présentateur de chèques à la compensation.

2.4. Vocabulaire

Par simplification, le terme « établissement » utilisé dans le rapport d'autoévaluation de la sécurité du chèque désigne le déclarant. Celui-ci est identifié par son code banque (code à 5 caractères du Fichier des Implantations Bancaires de la Banque de France).

Le vocabulaire du questionnaire d'évaluation est celui des concepts développés dans le RSC. **Ainsi, le glossaire du RSC est applicable.** De même, le « Système de Paiement par Chèque » correspond à l'ensemble des fonctions mises en œuvre dans la filière chèque au sens large. Pour une bonne appréhension des opérations concernées, il est important pour les établissements de bien cerner les activités qu'ils exercent dans chaque fonction.

Le terme « Remettant ONEGATE » désigne l'acteur autorisé à compléter le formulaire en mode saisie pour lui-même ou pour le compte de tiers.

Le terme « OSCAMPS » désigne l'application *back-end* de la Banque de France qui permet de stocker et d'analyser les données des collectes pour le compte de l'IEOM.

2.5. Calendrier prévisionnel

La périodicité de la collecte RSC est annuelle. La collecte annuelle des autoévaluations au RSC a généralement lieu au printemps de l'année n+1 pour dresser un bilan de l'année n. Les remettants ONEGATE accrédités pour le compte des établissements déclarants sont avertis chaque année par un courriel de lancement des dates officielles de période de collecte.

3. FONCTIONNEMENT DE LA COLLECTE

3.1. Désignation des remettants

Le déclarant a désigné un ou plusieurs remettants pour procéder aux déclarations et les valider (par exemple, un correspondant du métier saisit et un correspondant du contrôle permanent valide). Chacun de ces remettants est titulaire d'une accréditation qui lui permet de s'authentifier lors de sa connexion à ONEGATE-OSCAMPS.

3.2. Principes d'accréditation d'un remettant

La phase d'accréditation permet de vérifier que les remettants sont bien habilités par les déclarants à échanger des informations avec l'IEOM via les outils mis à disposition par la Banque de France. L'accréditation à ONEGATE est une procédure obligatoire sans laquelle il n'est pas possible de remettre des déclarations.

L'accréditation ne concerne que les remettants.

Pour un remettant qui n'a pas de compte sous ONEGATE, les demandes d'accréditation sont à réaliser sur la page onegate.banque-France.fr (« je n'ai pas de compte ») en sélectionnant la **collecte OSCAMPS IEOM** et chacun du(des) **code(s) LEI** des déclarants (ajouter, puis valider).

Pour un remettant déjà habilité sous ONEGATE, il conviendra de demander une extension de droits sur votre profil ONEGATE, en sélectionnant la **collecte OSCAMPS IEOM** et chacun du(des) **code(s) LEI** des déclarants (ajouter, puis valider).

Un mode opératoire précisant les modalités à suivre au titre des demandes d'extension de droits sur la collecte OSCAMPS est disponible dans le « Guide Remettant ONEGATE ».

Les notifications au remettant sont adressées si l'onglet contact du profil contient au moins une adresse e-mail valide pour laquelle les notifications sont activées.

Pour tout complément, la documentation ONEGATE (dont le guide au remettant) peut être demandée auprès des agences de l'IEOM.

Les règles générales permettent d'assurer la cohérence du futur système d'information :

- Aucune remise ne sera acceptée d'un remettant non accrédité à ONEGATE ;
- Si un remettant, accrédité à ONEGATE, remet des déclarations relatives à des déclarants pour lesquels il n'a pas été accrédité, celles-ci seront rejetées.

3.3. Modalités d'accès au questionnaire et canaux de transmission

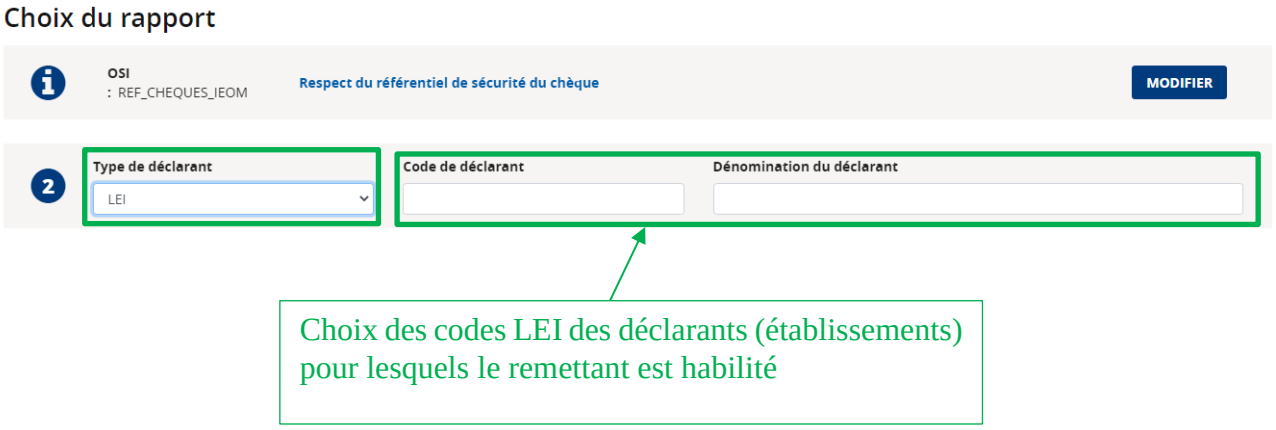
Le rapport d'autoévaluation est accessible en ligne sur le portail Internet sécurisé « ONEGATE » de la Banque de France :

- Accès à l'environnement de production : onegate.banque-France.fr

Le seul mode de remise accepté pour la collecte RSC est la saisie en ligne via le guichet ONEGATE (« canal U2A – Saisie en ligne » pour *User to Application*).

3.4. Description de l'accès au questionnaire de la collecte

Le menu « Rapports » permet de visualiser les enquêtes auxquelles le remettant ONEGATE, agissant pour le compte du déclarant, doit répondre. Est affiché dans cette liste, sous le domaine OSI, le rapport REF_CHEQUES_IEOM au libellé long « Respect du référentiel de sécurité du chèque ».

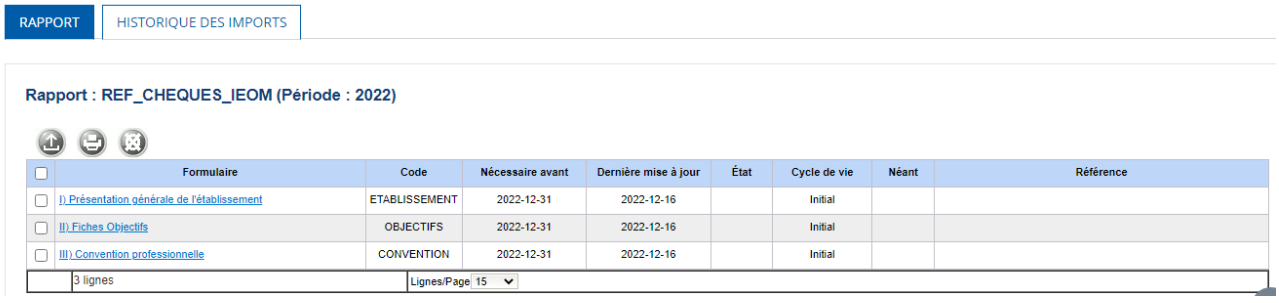


Choix des codes LEI des déclarants (établissements) pour lesquels le remettant est habilité

4. DESCRIPTION DES RÉPONSES AU RAPPORT D'AUTOÉVALUATION DE LA SÉCURITÉ DU CHÈQUE

4.1. Écran d'accueil et choix des sections

Le rapport d'autoévaluation est composé de 3 parties présentées dans l'écran d'accueil



4.2. Partie 1 : Présentation générale de l'établissement

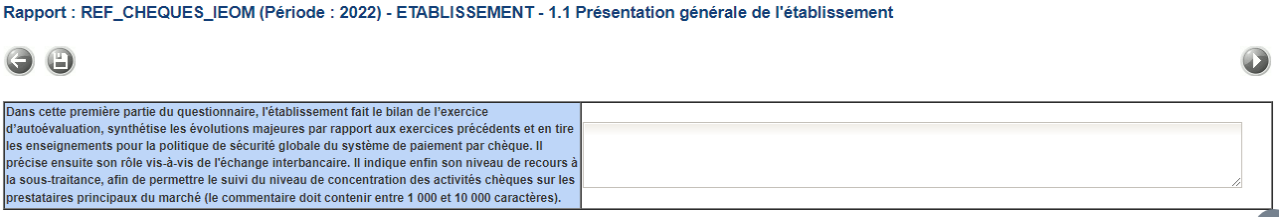
Cette partie est composée des items suivants.

4.2.1. Présentation générale de l'établissement

L'appréciation synthétique est obligatoirement renseignée par le déclarant. Elle fait le bilan de l'exercice d'autoévaluation, synthétise les évolutions majeures par rapport aux exercices précédents et en tire les enseignements pour la politique de sécurité globale du système de paiement par chèques.

Elle permet au déclarant d'appeler l'attention de l'IEOM sur tout sujet qu'il juge utile de mentionner pour appréhender les résultats de son exercice d'autoévaluation.

L'écran à compléter est présenté ci-dessous :



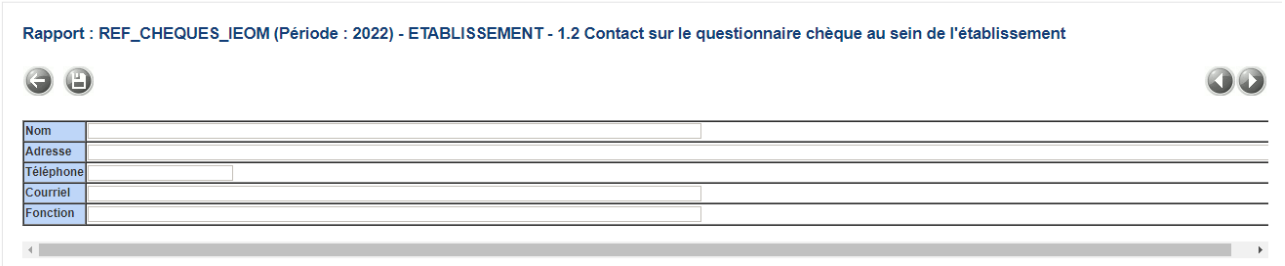
Description des contraintes et contrôles de la section

- Le commentaire saisi doit contenir entre 1000 et 4 000 caractères.
- Si le commentaire obligatoire est inférieur à 1000 caractères, le déclarant a le message d'erreur « commentaire saisi doit contenir au moins 1000 caractères ».
- Si le commentaire obligatoire est supérieur à 4 000 caractères, le déclarant a le message d'erreur « commentaire saisi ne doit pas contenir plus de 4 000 caractères ».

4.2.2. Contact sur le questionnaire chèque au sein de l'établissement

Le déclarant a désigné une personne pouvant être contactée par l'IEOM pour toute question sur la sécurité du chèque au sein de l'établissement. Cette personne peut être différente du (des) remettant(s) accrédité(s) pour effectuer la déclaration de l'autoévaluation.

Ses coordonnées et sa fonction sont renseignées dans l'écran ci-dessous.



Description des contraintes et contrôles de la section

- Chaque libellé affiché doit être obligatoirement renseigné. L'absence de saisie d'un ou de plusieurs libellés affichés génère un message d'erreur « champ(s) manquant(s) » empêchant la validation finale du document.

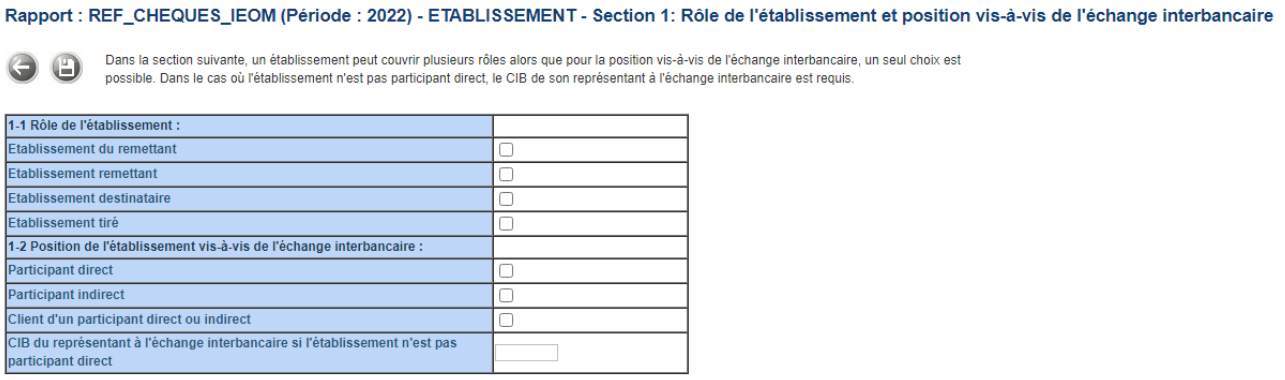
4.2.3. Rôle de l'établissement et position vis-à-vis de l'échange interbancaire

Cette section permet au déclarant de définir son rôle au sein du système de paiement par chèque. Les réponses se font par l'intermédiaire de cases à cocher.

Un établissement peut couvrir plusieurs rôles voire les quatre rôles.

Pour la position vis-à-vis de l'échange interbancaire, un seul choix est possible. Si le déclarant n'est pas participant direct, il doit compléter le CIB de son participant direct. Un établissement ayant coché uniquement « Établissement du remettant », ne peut pas cocher la position « Participant direct » ou « Participant indirect ». En revanche, si un établissement cumule le rôle « Établissement du remettant » avec celui d'« Établissement remettant », il devra cocher une position « Participant direct » ou « Participant indirect ».

L'écran à compléter est présenté ci-dessous :



Description des contraintes et contrôles de la section

- Au minimum une case de « Rôle de l'établissement » doit être indiquée par l'établissement. L'absence de choix d'un libellé affiché génère un message d'erreur « Vous devez définir votre rôle au sein de l'échange interbancaire. » empêchant la validation finale du document.
- Au minimum une réponse doit être cochée par le déclarant dans « Position de l'établissement ». L'absence de choix d'un libellé affiché génère un message d'erreur « Vous devez cocher une case unique concernant la position de votre établissement vis-à-vis de l'échange interbancaire. » empêchant la validation finale du document

4.3. Répartition des principaux traitements et de la sous-traitance

Dans cette section, l'établissement précise, au cours de l'année sous revue, ses modalités d'organisation pour cinq fonctions : (1) la fabrication et l'impression des fonds de chèque, (2) la personnalisation et le façonnage des chéquiers, (3) la distribution des chéquiers aux clients, (4) la dématérialisation des chèques remis à l'encaissement et (5) l'archivage à long-terme des vignettes.

L'établissement déclarant doit compléter pour chacune de ces fonctions :

- La part de la fonction réalisée par lui-même (internalisation) ;
- La part de la fonction réalisée par des prestataires bancaires internes ou externes au groupe (sous-traitance auprès d'autres établissements bancaires agréés par l'ACPR), en précisant alors le code interbancaire (CIB) de ce prestataire bancaire ;

- La part de la fonction réalisée par des prestataires non bancaires (sous-traitance auprès de prestataires non bancaires), en renseignant la raison sociale et le SIREN / RIDET / n° de TAHITI du prestataire en fonction de son implantation. Les prestataires non bancaires et/ou non français sont à référencer avec leur LEI.

Pour chaque acteur participant à l'une ou plusieurs de ces cinq fonctions de l'établissement, le déclarant doit renseigner son identité, préciser s'il appartient au groupe ou réseau bancaire du déclarant (*Groupe – G - ou Hors Groupe – HG*) et sa contribution en % à la fonction. Pour cette dernière, les valeurs attendues, à défaut d'être exactes, sont à exprimer en pourcentage du volume total des traitements réalisés pour le compte de l'établissement déclarant. Elle consiste en un nombre entier de 0 à 100, sans signe %.

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit ainsi s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou étranger. Dans la mesure du possible, l'établissement déclare les sous-traitants directement en charge de la fonction, y compris si ceux-ci sont eux-mêmes des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.1. Description de la section « IMPRESSION »

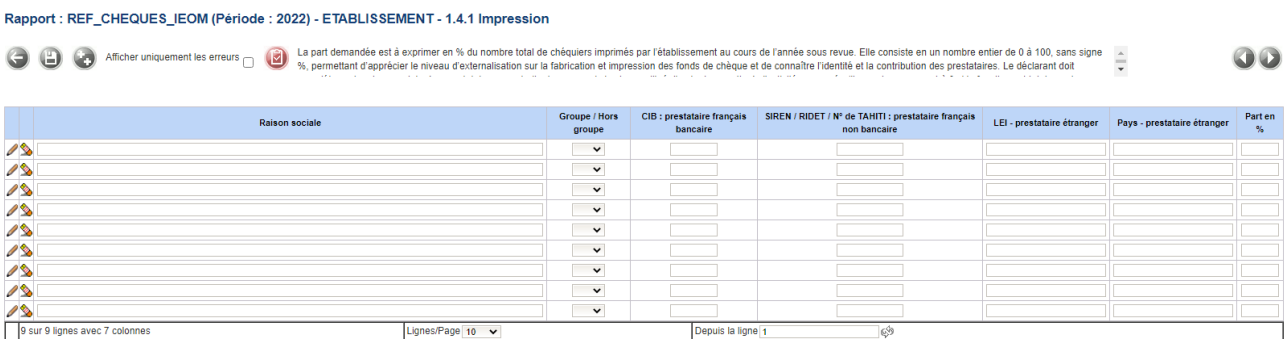
Il s'agit d'apprécier le niveau d'externalisation, y compris auprès de prestataires internes au groupe ou réseau bancaire, sur la fabrication et l'impression des fonds de chèques et de connaître l'identité et la contribution des différents prestataires. La part demandée est à exprimer en % du nombre total de chéquiers imprimés par l'établissement au cours de l'année sous revue.

La part demandée consiste en un nombre entier de 0 à 100, sans signe %, permettant d'apprécier le niveau d'externalisation sur la fabrication et l'impression des fonds de chèque et de connaître l'identité et la contribution des prestataires. Le déclarant doit compléter :

- La raison sociale des prestataires sous-traitants, y compris la sienne s'il réalise tout ou partie de l'activité concernée (il renseigne une part à 0 si la fonction est totalement externalisée),
- Un CIB (si le sous-traitant est un prestataire de service de paiement français), ou un SIREN (si le sous-traitant est une entreprise non bancaire située en France ou dans les départements d'Outre-Mer), ou un RIDET ou un N° de Tahiti (si le sous-traitant est une entreprise située dans une collectivité française du Pacifique) ou un LEI et un pays si le prestataire est situé à l'étranger.

Le déclarant doit préciser pour chaque prestataire s'il fait partie ou non de son groupe bancaire ou réseau bancaire (Groupe – G - ou Hors Groupe – HG -).

Le déclarant doit s'assurer que le total de la fonction, en additionnant les contributions des prestataires concernés (y compris la part réalisée par le déclarant lui-même), est égal à 100 (100%).



Description des contraintes et contrôles de la section

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou à l'étranger. Dans la mesure du possible, l'établissement déclare les sous-traitants directement en charge de la fonction, y compris si ceux-ci sont des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.2. Description de la section « PERSONNALISATION »

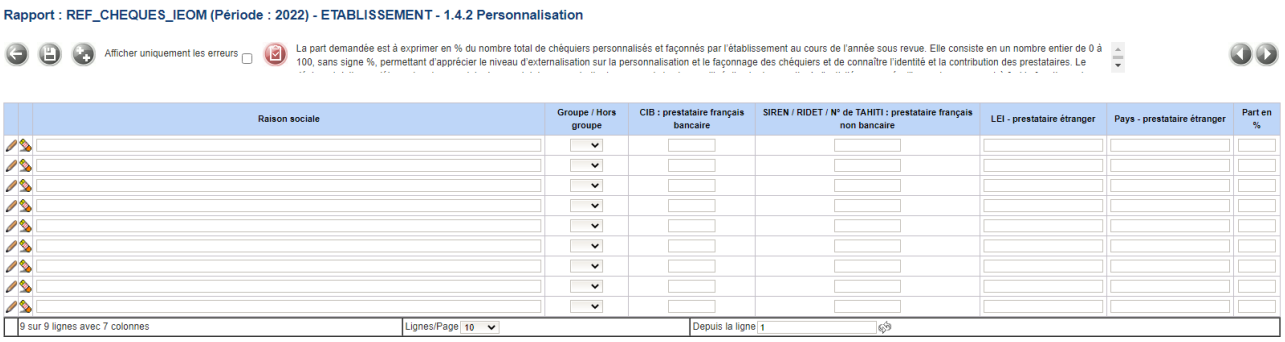
Il s'agit d'apprécier le niveau d'externalisation, y compris auprès de prestataires internes au groupe ou réseau bancaire, sur la personnalisation et le façonnage des chéquiers et de connaître l'identité et la contribution de ses différents prestataires. La part demandée est à exprimer en % du nombre total de chéquiers personnalisés et façonnés par l'établissement au cours de l'année sous revue.

La part demandée consiste en un nombre entier de 0 à 100, sans signe %, permettant d'apprécier le niveau d'externalisation sur la personnalisation et le façonnage des chéquiers et de connaître l'identité et la contribution des prestataires. Le déclarant doit compléter :

- La raison sociale des prestataires sous-traitants, y compris la sienne s'il réalise tout ou partie de l'activité concernée (il renseigne une part à 0 si la fonction est totalement externalisée),
- Un CIB (si le sous-traitant est un prestataire de service de paiement français), ou un SIREN (si le sous-traitant est une entreprise située en France ou dans les départements d'Outre-Mer), ou un RIDET ou un N° de Tahiti (si le sous-traitant est une entreprise située dans une collectivité française du Pacifique) ou un LEI et un pays si le prestataire est situé à l'étranger.

Le déclarant doit préciser pour chaque prestataire s'il fait partie ou non de son groupe bancaire ou réseau bancaire (Groupe – G - ou Hors Groupe – HG -).

Le déclarant doit s'assurer que le total de la fonction, en additionnant les contributions des prestataires concernés (y compris la part réalisée par le déclarant lui-même), est égal à 100 (100%).



Description des contraintes et contrôles de la section

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit ainsi s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou à l'étranger. Dans la mesure du possible, l'établissement déclare les sous-

traitants directement en charge de la fonction, y compris si ceux-ci sont des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.3 Description de la section « DISTRIBUTION »

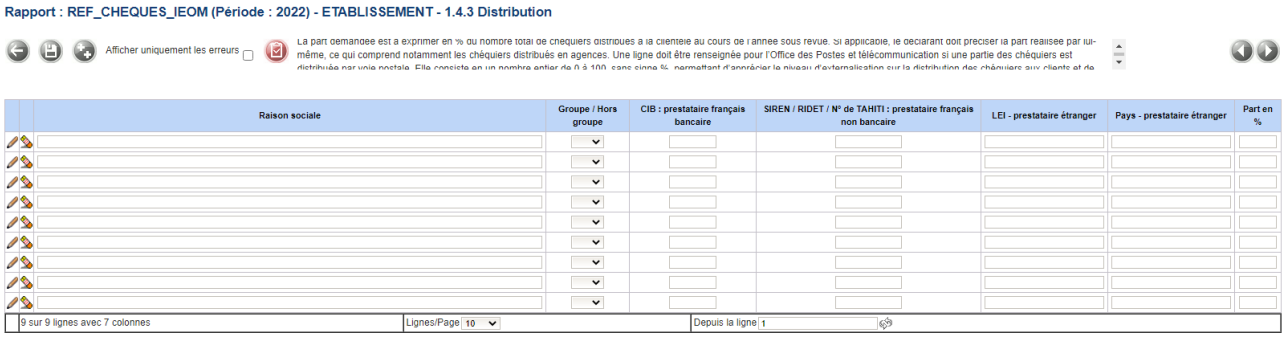
Il s'agit d'apprécier le niveau d'externalisation, y compris auprès de prestataires internes au groupe ou réseau bancaire, sur la fonction de distribution et de remise des chéquiers aux clients, c'est-à-dire le dernier maillon de la chaîne de fabrication et de mise à disposition des chéquiers et de connaître l'identité et la contribution de ses différents prestataires. La part demandée est à exprimer en % du nombre total de chéquiers distribués à sa clientèle au cours de l'année sous revue. Si applicable, le déclarant doit préciser la part réalisée par lui-même, ce qui comprend notamment les chéquiers distribués en agences. Une ligne doit être renseignée pour l'Office des Postes et télécommunication si une partie des chéquiers est distribuée par voie postale.

La part demandée consiste en un nombre entier de 0 à 100, sans signe %, permettant d'apprécier le niveau d'externalisation sur la distribution des chéquiers aux clients et de connaître l'identité et la contribution des prestataires. Le déclarant doit compléter :

- La raison sociale des prestataires sous-traitants, y compris la sienne s'il réalise tout ou partie de l'activité concernée (il renseigne une part à 0 si la fonction est totalement externalisée),
- Un CIB (si le sous-traitant est un prestataire de service de paiement français), ou un SIREN (si le sous-traitant est une entreprise située en France ou dans les départements d'Outre-Mer), ou un RIDET ou un N° de Tahiti (si le sous-traitant est une entreprise située dans une collectivité française du Pacifique) ou un LEI et un pays si le prestataire est situé à l'étranger.

Le déclarant doit préciser pour chaque prestataire s'il fait partie ou non de son groupe bancaire ou réseau bancaire (Groupe – G - ou Hors Groupe – HG -).

Le déclarant doit s'assurer que le total de la fonction, en additionnant les contributions des prestataires concernés (y compris la part réalisée par le déclarant lui-même), est égal à 100 (100%).



Description des contraintes et contrôles de la section

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit ainsi s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou étranger. Dans la mesure du possible, l'établissement déclare les sous-traitants directement en charge de la fonction, y compris si ceux-ci sont des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.4. Description de la section « DEMATERIALISATION »

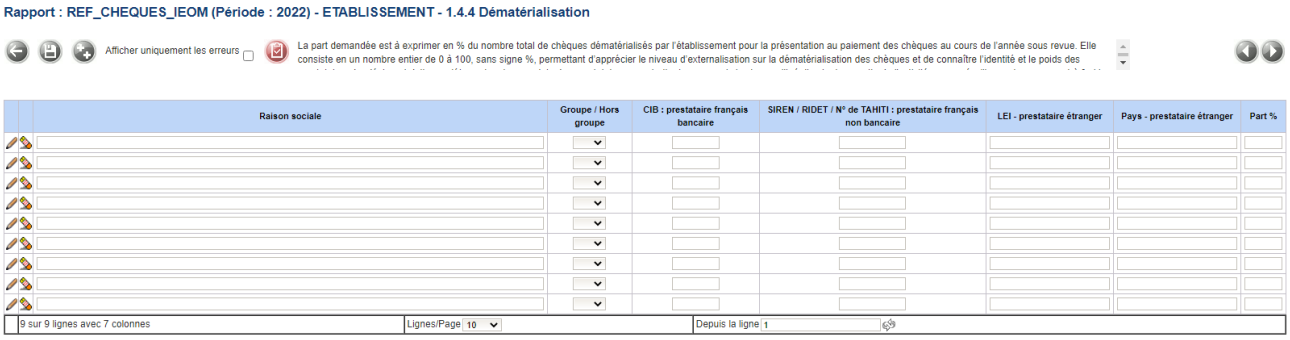
Il s'agit d'apprécier le niveau d'externalisation, y compris auprès de prestataires internes au groupe ou réseau bancaire, sur la dématérialisation des chèques et de connaître l'identité et la contribution de ses différents prestataires. La dématérialisation pour le compte de l'établissement remettant comprend « *la réception des chèques, le contrôle de leur conformité, la réception de fichiers d'ajustement, la capture des données du chèque, la réconciliation, la reproduction recto verso, l'ajout des montants et ajustement du lot traité, la constitution éventuelle de l'image-chèque, la constitution du fichier de remise destiné aux systèmes d'échange et de compensation et la détermination des chèques circulants, notamment la circulation aléatoire* ». La part demandée est à exprimer en % du nombre total de chèques dématérialisés par l'établissement pour la présentation au paiement des chèques au cours de l'année sous revue.

La part demandée consiste en un nombre entier de 0 à 100, sans signe %, permettant d'apprécier le niveau d'externalisation sur la dématérialisation des chèques et de connaître l'identité et le poids des prestataires. Le déclarant doit compléter :

- La raison sociale des prestataires sous-traitants, y compris la sienne s'il réalise tout ou partie de l'activité concernée (il renseigne une part à 0 si la fonction est totalement externalisée),
- Un CIB (si le sous-traitant est un prestataire de service de paiement français), ou un SIREN (si le sous-traitant est une entreprise située en France ou dans les départements d'Outre-Mer), ou un RIDET ou un N° de Tahiti (si le sous-traitant est une entreprise située dans une collectivité française du Pacifique) ou un LEI et un pays si le prestataire est situé à l'étranger.

Le déclarant doit préciser pour chaque prestataire s'il fait partie ou non de son groupe bancaire ou réseau bancaire (Groupe – G - ou Hors Groupe – HG -).

Le déclarant doit s'assurer que le total de la fonction, en additionnant les contributions des prestataires concernés (y compris la part réalisée par le déclarant lui-même), est égal à 100 (100%).



<u>Description des contraintes et contrôles de la section</u>

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit ainsi s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou étranger. Dans la mesure du possible, l'établissement déclare les sous-traitants directement en charge de la fonction, y compris si ceux-ci sont des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.5. Description de la section « ARCHIVAGE »

Il s'agit d'apprécier le niveau d'externalisation, y compris auprès de prestataires internes au groupe ou réseau bancaire, sur l'archivage à long terme des vignettes (au-delà des 60 jours et jusqu'à 10 ans), dont l'établissement a la charge en tant qu'établissement remettant ou en tant qu'établissement tiré. La part

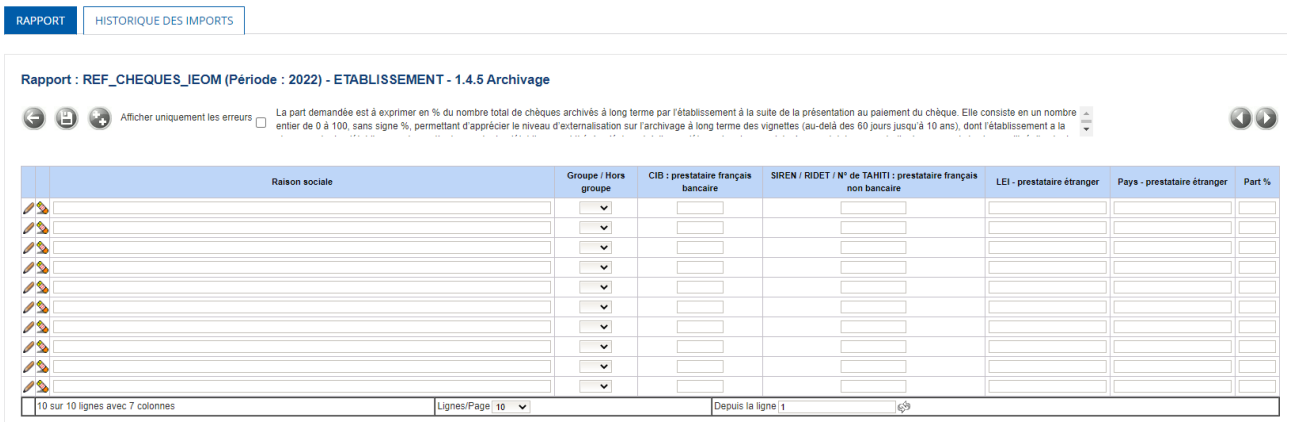
demandée est à exprimer en % du nombre total de chèques archivés à long terme par l'établissement à la suite de la présentation au paiement du chèque.

La part demandée consiste en un nombre entier de 0 à 100, sans signe %, permettant d'apprécier le niveau d'externalisation sur l'archivage à long terme des vignettes (au-delà des 60 jours jusqu'à 10 ans), dont l'établissement a la charge en tant qu'établissement remettant ou en tant qu'établissement tiré. Le déclarant doit compléter :

- La raison sociale des prestataires sous-traitants, y compris la sienne s'il réalise tout ou partie de l'activité concernée (il renseigne une part à 0 si la fonction est totalement externalisée),
- Un CIB (si le sous-traitant est un prestataire de service de paiement français), ou un SIREN (si le sous-traitant est une entreprise située en France ou dans les départements d'Outre-Mer), ou un RIDET ou un N° de Tahiti (si le sous-traitant est une entreprise située dans une collectivité française du Pacifique) ou un LEI et un pays si le prestataire est situé à l'étranger.

Le déclarant doit préciser pour chaque prestataire s'il fait partie ou non de son groupe bancaire ou réseau bancaire (Groupe – G - ou Hors Groupe – HG -).

Le déclarant doit s'assurer que le total de la fonction, en additionnant les contributions des prestataires concernés (y compris la part réalisée par le déclarant lui-même), est égal à 100 (100%).



Description des contraintes et contrôles de la section

Le total des contributions des différents acteurs doit être égal à 100% pour chaque fonction. Le déclarant doit ainsi s'assurer que le total des contributions, en additionnant les contributions des prestataires et la part internalisée dans l'établissement, est égal à 100 (100%).

Tout sous-traitant doit être renseigné, que celui-ci soit bancaire ou non bancaire, interne ou externe au groupe, français ou étranger. Dans la mesure du possible, l'établissement déclare les sous-traitants directement en charge de la fonction, y compris si ceux-ci sont des sous-traitants des prestataires avec lequel l'établissement déclarant est lié par un contrat.

4.3.6. Description de la section COMMENTAIRES

Le déclarant peut faire un commentaire à propos de l'organisation de ses principaux traitements et de la sous-traitance. Si le déclarant fait le choix de saisir un commentaire, sa longueur doit rester inférieure à 4 000 caractères. Il s'agit d'informer l'IEOM sur toute évolution ou projet majeur intervenu au cours de l'exercice (ex : nouvelle externalisation, changement de prestataire etc.)

Description des contraintes et contrôles de la section

- Si un commentaire est saisi, il doit contenir moins de 4 000 caractères.
- Si le commentaire est supérieur à 4 000 caractères, nous avons le message d'erreur « commentaire saisi ne doit pas contenir plus de 4 000 caractères ».

4.4. Partie 2 : Fiches Objectifs de sécurité

La partie Fiches Objectifs de sécurité est constituée par l'autoévaluation des 9 objectifs de sécurité du RSC par les déclarants.

Une « fiche objectif » affiche un objectif cible qui est caractérisé par des **considérations clés (CC).** Chaque CC est composée de critères d'autoévaluation a), b), c) etc. et d'un tableau de correspondance permettant à l'établissement de s'autoévaluer. Le questionnaire d'autoévaluation est repris dans le fichier Excel joint en annexe « *IEOM RSC Objectifs Sécurité & Considérations clés* » et permet de préparer la déclaration.

Ainsi, pour chaque CC, l'évaluation s'articule en trois étapes :

❶ Réponse aux critères d'autoévaluation : le critère est-il satisfait ou non ?

❷ Évaluation du niveau de couverture : le niveau est déterminé selon le nombre de réponses positives aux critères, conformément au tableau de correspondance fourni pour chaque CC.

❸ Report de l'autoévaluation : le niveau de couverture est reporté sur l'échelle de 1 à 4.

Les 9 objectifs de sécurité devant être évalués :

1	Gouvernance et organisation	Compte tenu des interactions et des interdépendances au sein du SPC, la sécurité globale est conditionnée par une coopération réelle et efficace entre les acteurs. À partir de ce fondement, la gouvernance de la sécurité vise à assurer que les mesures de sécurité sont en place et restent à tout moment optimales et appropriées. Les acteurs doivent disposer d'un ensemble documentaire formalisé et régulièrement mis à jour définissant ce cadre de gouvernance et l'organisation de la sécurité du SPC.
2	Evaluation des risques	La gestion de la sécurité repose sur l'identification des actifs à protéger associée à une analyse des risques encourus ainsi qu'à la mise en place de mesures organisationnelles, techniques et procédurales en vue d'assurer cette protection. Elle prévoit une évaluation périodique des mesures déployées en vue de leur efficacité.
3	Contrôle et encadrement des risques	Les acteurs doivent mettre en œuvre des mesures de sécurité adéquates en vue d'encadrer les risques identifiés, en conformité avec la politique de sécurité de la filière et leur politique de sécurité globale du chèque.
4	Gestion des incidents et reporting	Les acteurs doivent disposer d'un système de surveillance des incidents relatifs aux opérations par chèque et aux réclamations des clients qui permettent un recensement exhaustif des incidents. En fonction de leur niveau de gravité, ce système de surveillance doit comprendre une procédure de remontée des incidents qui produise une information adéquate auprès des instances de gouvernance de l'établissement, auprès des parties prenantes externes concernées, et pour les incidents graves auprès de la Banque de France.
5	Traçabilité – piste d'audit	Les acteurs doivent mettre en place un processus permettant une traçabilité destinée à alimenter une piste d'audit ininterrompue pour chacune des opérations couvertes par le SPC.
6	Sécurité physique du chèque	Les acteurs s'assurent de la sécurité physique des chèques tout au long de leur cycle de vie.
7	Sécurité des environnements des opérations	Les environnements physique et logique du SPC sont sécurisés, et permettent d'assurer la protection des supports physiques et logiques ainsi que des opérations exercées. Ils garantissent la qualité, la disponibilité et l'exploitabilité technique des éléments archivés.
8	Dispositif de surveillance des opérations et de prévention de la fraude	La surveillance des opérations vise à prévenir, détecter et bloquer les tentatives d'encaissement ou de paiement suspectées d'être d'origine frauduleuse ou irrégulière. Cette surveillance doit être encadrée par des procédures formalisées définissant les règles et typologies d'alertes. Le dispositif de surveillance est actualisé régulièrement afin de prendre en compte toute évolution des risques.
9	Sensibilisation des clients aux règles de sécurité	Les établissements veillent à la sensibilisation de leurs clients aux règles de vigilance relatives à la conservation d'une formule prémarquée, l'émission ou la réception d'un chèque, sa conservation et sa remise à l'encaissement.

4.4.1. Remarques générales

Les objectifs de sécurité ne sont pas des règles impératives ; ils correspondent aux critères d'évaluation pour lesquels est attendue une image de la situation réelle et non une cotation maximale sur tous les objectifs.

L'autoévaluation doit respecter quelques principes généraux. Ainsi, pour bon nombre d'objectifs, la démarche en matière d'analyse de risque suppose qu'une **analyse préalable** des différents processus de traitement ou de gestion du chèque soit réalisée. Le RSC fournit une base d'analyse de risques, mais celle-ci peut être menée selon les critères propres de l'établissement. À partir de ce socle, certains critères peuvent être ajoutés, selon les organisations concernées et leur appréciation du risque. **Quelle que soit la méthode d'analyse privilégiée par l'établissement, tous les critères précisés dans le questionnaire doivent être pris en compte.**

4.4.2. Les appréciations communes à l'ensemble des critères

Ne nous concerne pas (NNCP)

Ce choix signifie que l'activité sur laquelle porte la question n'est pas exercée par l'établissement, directement ou indirectement (ex : un déclarant qui n'est pas établissement tiré cochera cette case pour la considération-clé 8.2 de l'objectif 8 « Dispositif de surveillance des opérations et de prévention de la fraude »).

Une réponse NNCP doit nécessairement s'accompagner d'un commentaire explicatif.

En aucun cas la réponse NNCP ne peut signifier que l'activité est externalisée auprès d'un prestataire externe ou d'une entité commune au sein d'un groupement. Dans ces deux situations, l'établissement doit fournir une note d'évaluation à partir d'éléments qu'il détient ou qui lui ont été communiqués par l'entité exerçant l'activité pour son compte.

Incident grave

L'incident grave s'interprète comme l'incapacité de rendre le service attendu, qui touche un nombre important d'opérations, en volume et en valeur, et qui a des **conséquences pour l'établissement** et/ou les autres acteurs du système de paiement par chèques, en termes juridiques, d'image, opérationnels, financiers. Ce type d'incidents est susceptible de générer des retards, des coûts, des pertes ; il ne s'agit pas des incidents d'exploitation courants.

Les critères d'identification des incidents graves sur le système de paiement par chèque sont précisés dans l'annexe au RSC « *IEOM RSC Annexe Identification notification des incidents graves chèque* ». Ces critères communs doivent au minimum être pris en compte et déclinés dans les procédures de l'établissement, mais ce dernier peut les compléter ou les préciser.

Augmentation significative de la fraude

L'augmentation significative de la fraude s'apprécie comme une évolution défavorable et importante au cours de l'exercice évalué des cas et/ou des montants de fraude au chèque, tels que recensés par l'établissement puis déclarés à l'IEOM dans le cadre de la collecte « *Recensement de la fraude aux moyens de paiement scripturaux* », sur une ou plusieurs des typologies définies de fraude au chèque. **Elle peut par exemple être comprise comme une hausse supérieure à 10% par rapport à l'exercice précédent.**

Commentaire sur l'évaluation

Chaque considération clé comporte une partie « Commentaire sur l'évaluation » Cette partie doit être systématiquement complétée par l'établissement, afin d'expliquer les raisons principales sous-tendant les résultats de son évaluation, pour :

- chaque situation de type NNCP ;
- chaque considération clé pour laquelle l'évaluation ne conclut pas à une pleine conformité (notation 1, 2 ou 3) ;
- chaque considération clé pour laquelle l'évaluation a évolué d'une année sur l'autre à la hausse comme à la baisse (y compris lorsque la notation est montée à 4).

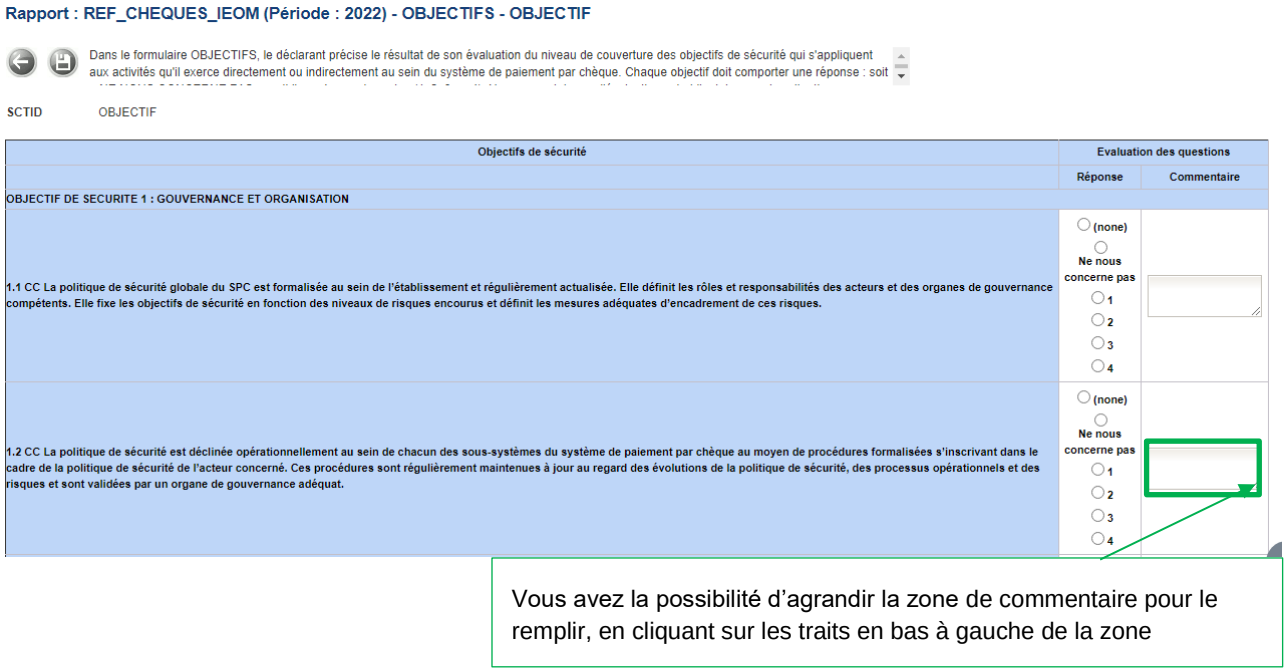
Ce commentaire doit être précis et synthétique.

4.4.3. Les fiches Objectifs de sécurité – Considérations Clés

Cette partie a principalement pour objet d'aider à la compréhension des critères d'autoévaluation des considérations clés. Le déclarant pourra utilement se référer aux communications adhérents du CFONB visées dans les explications, prises sous forme de recommandations applicables à la filière chèque.

Un exemple de la section Objectifs est présenté ci-dessous :

Un exemple de la section Objectifs est présenté ci-dessous :



Description des contraintes et contrôles de la section

- Le commentaire saisi doit contenir entre 200 et 1 000 caractères.
    - Si le nombre de caractères est inférieur à 200 caractères, le message suivant apparaît : « Le commentaire saisi doit contenir au moins 200 caractères »
    - Si le nombre de caractères est supérieur à 1 000 caractères, le message suivant apparaît : « Le commentaire saisi ne doit pas contenir plus de 1 000 caractères »
- Si réponse = « NNCP », «1», «2» ou «3», un commentaire est obligatoire. Si cette règle n'est pas respectée, le message d'erreur suivant apparaît « Commentaire obligatoire si réponse à NNCP, 1 ,2 ou 3».
- Si réponse = « 4 », une pop up d'avertissement apparaît avec le message suivant « Si la note 4 est apposée pour la 1ère année, merci de compléter un commentaire justifiant cette notation ».

Objectifs 1 à 5 - Gouvernance de la sécurité et dispositifs de contrôle

Ces cinq objectifs ne portent pas sur le fonctionnement des instances de pilotage de la Place mais sur la gouvernance globale de la sécurité du chèque de l'établissement. Ces objectifs fixent des exigences portant **sur l'ensemble des processus liés au Système de Paiement par Chèque**. Ils visent à s'assurer que l'établissement déclarant a mis en place de façon effective un cadre de gouvernance d'ensemble de la sécurité des opérations qu'il exerce ou dont il a la responsabilité au sein du système de paiement par chèque.

Au travers de ces objectifs, le déclarant doit par ailleurs évaluer la mesure de sa participation aux instances de Place dans quatre domaines : i/ sa coopération aux principes de bon fonctionnement de la filière chèque, ii/ sa participation aux tests de Place, iii/ l'exercice d'une veille en matière de sécurité, iv/ la transmission d'alertes en cas de besoin.

OBJECTIF 1 : Une organisation et des objectifs bien définis et documentés, à la fois en interne et dans les relations de l'établissement avec des tierces parties.

« *La sécurité globale étant conditionnée par une coopération réelle et efficace entre les acteurs* ». Il convient pour le déclarant de se tenir informé ou de participer aux travaux interbancaires et de se conformer, le cas échéant, aux procédures et aux décisions prises par les instances locales en matière de chèque.

CC 1.1. critère a) :

- L'ensemble des opérations chèque est pris en compte dans la politique de sécurité, mais celle-ci peut être intégrée à d'autres politiques internes. En matière de système d'information par exemple, la politique de sécurité des processus liés au chèque peut être la même que pour les autres moyens de paiement, si le système d'information est commun.

CC 1.1. critère b) :

- S'agissant de l'instance de gouvernance, l'IEOM considère que l'administration de la sécurité doit être entendue au sens large, c'est-à-dire qu'elle se rapporte à l'ensemble des opérations liées à la filière chèque, quel qu'en soit l'objet (accès, locaux, transports, valeurs, systèmes d'information etc.). L'IEOM n'entend pas ainsi figer un principe d'organisation dans les établissements, mais veut préserver une notion de vision globale et de coordination, à un niveau hiérarchique adapté, sans toutefois préjuger de ce niveau. Il appartient à cette instance de gouvernance de mettre en œuvre l'organisation la plus efficace possible et de prévoir les éléments de contrôle interne qui permettent de mesurer la bonne application de la politique de sécurité (objectif de sécurité 3).
- En général, l'instance de gouvernance ayant validé la politique de sécurité du chèque (considération clé 1.1) est la même que celle visée pour la validation des procédures (considération clé 1.2), la validation de la cartographie des risques (considération clé 2.1), la revue des indicateurs relatifs aux incidents, aux réclamations des clients et à la fraude (considération 4.1) et pour la revue et la validation du plan de continuité des activités (considération clé 4.2).

CC 1.2. critère b) :

- S'agissant de l'organe de gouvernance, il s'agit généralement de l'instance de gouvernance mentionnée dans le critère b de la CC 1.1. L'organe compétent pour la validation des procédures de sécurité devrait également avoir une compétence pour fournir des moyens nécessaires à la mise en œuvre de ces procédures.

CC 1.3. critère a) :

- La formalisation mentionnée renvoie à une convention participant direct/participant indirect. Cela étant, les liens entre membres d'un même groupe ou entre une maison mère et ses filiales ne justifient pas de mettre en place un cadre contractuel aussi formalisé que pour une relation de prestation de service (représentation au système d'échange) hors groupe.

OBJECTIF 2 : Un processus régulier d'évaluation des risques et de définition des mesures de protection adaptées

CC 2.2. :

- La veille sécurité consiste à se tenir pro-activement informé de ce qui pourrait provoquer des incidents (nouvelles technologies, nouveaux types de fraude …) et à faire face aux problèmes

de sécurité qui pourraient se poser (notion de prévention). À titre d'exemple, l'activité de veille peut être matérialisée par la prise d'informations dans les médias spécialisés (articles de presse, sites internet), par la participation à des groupes de Place ou par des contacts avec des fournisseurs.

- Cette activité est exercée par l'établissement lui-même, de manière centralisée ou non, ou par un autre acteur qui le tient informé.

OBJECTIF 3 : Un dispositif de contrôle des opérations permettant d'assurer la bonne maîtrise des risques identifiés

CC 3.1. critère a) :

- Il s'agit de tests d'importance décidés par l'instance de pilotage (CFONB, FBF) concernant la mise en œuvre de nouvelles procédures par exemple. Ces tests de Place concernent les participants directs, les participants indirects et d'éventuels autres établissements.

CC 3.1. critère c) :

- Il ne s'agit pas d'avoir un plan d'audit dédié à chaque activité exercée. Des solutions consistant en des plans d'audit pluriannuels, des audits transversaux ou communs à plusieurs établissements sont tout à fait possibles.

OBJECTIF 4 : Un dispositif d'identification, de recensement et de réponse aux incidents opérationnels de sécurité complété par un dispositif de remontée des incidents aux instances de gouvernance et à l'IEOM pour ceux qui sont qualifiés comme « graves »;

CC 4.1. critère a) :

- S'agissant des « acteurs concernés en fonction du degré de criticité des incidents », il peut s'agir à la fois des acteurs internes (contrôle interne, audit, instance de gouvernance compétente pour le système de paiement par chèque, direction générale etc.) comme des acteurs externes (autres établissements, IEOM, GIE SIE, etc.).

CC 4.2. :

- Il est entendu qu'il n'y a pas nécessairement un seul plan de secours, mais un plan par activité, voire d'autres solutions.

OBJECTIF 5 : Une traçabilité complète des opérations, aux niveaux physique et logique

CC 5.1. :

- Il s'agit de couvrir l'ensemble de la filière chèque et des locaux.

CC 5.1. critère a) :

- Les analyses de besoins en matière de traçabilité ont généralement été effectuées au fur et à mesure de la mise en place des applications ou des modifications d'organisations.

Objectif 6 – Sécurité physique du chèque

Cet objectif vise à couvrir les risques spécifiques inhérents à la nature physique du chèque durant l'ensemble de son cycle de vie, de sa fabrication à sa destruction.

CC 6.1. : Le respect des normes en vigueur lors de la fabrication des formules de chèques.

critère a) :

- L'objectif vise les normes NF K 11-111 et NF K 11-112 et les recommandations des communications adhérents CFONB n° 1997/249 du 18 juin 1997 (la formule de chèque - Évolutions liées au passage à l'euro) et n° 2003/332 du 22 décembre 2003 (Norme NF K 11-111 - Composition de la zone interbancaire de la ligne magnétique CMC 7 des chèques). Le site public du CFONB présente également la liste des « *Ateliers de personnalisation ayant fourni l'attestation de conformité à la norme NF K11-112 avec complément d'information* ».

critère b) :

- Pour les chèques de banque, l'objectif vise les recommandations des communications adhérents n° 2022/0016 du 1er juin 2022 (dispositions relatives à la protection des chèques de banque – maintien du filigrane et information clientèle) et 2008/233 du 28 juillet 2008 (règles pour la production des chèques de banque avec filigrane – recommandation obligatoire depuis le 1er juillet 2009).

critère d) :

- Les recommandations professionnelles mentionnées sont celles de la communication adhérents n° 2012/144 du 25 juillet 2012 (établissement des lettres-chèques - Règles et recommandations du CFONB) et de la communication adhérents n° 2019/0015 du 21 mai 2019 – Règles et recommandations pour l'établissement des lettres-chèques – Rappel de règles – document destiné à la profession bancaire.

De façon générale, la protection des chèques ne s'applique pas spécifiquement aux zones variables ; elle peut être de même niveau sur l'ensemble de la formule.

CC 6.2. : Les risques de falsification et de contrefaçon de formules de chèques, qui constituent deux des catégories de fraude retenues dans la déclaration statistique de fraude à l'IEOM.

Il est attendu que l'établissement fasse le choix des éléments de sécurité qu'il intègre dans ses formules de chèques. Ces éléments de sécurité doivent permettre aux bénéficiaires et aux autres acteurs du système de paiement par chèque, notamment les établissements remettants et leurs prestataires, de mieux détecter les falsifications et les contrefaçons. Certains éléments de sécurité peuvent être connus et vérifiés par des personnes extérieures (ex: filigrane, motif fluorescent, micro-lettres…). D'autres n'ont pas vocation à être directement connus mais leur présence rend les tentatives de falsification plus visibles et donc plus facilement détectables (ex: papier, agent réactif…).

critère d) :

- Il ne s'agit pas de porter à la connaissance des bénéficiaires de chèque les secrets de fabrication des chèques mais de communiquer sur les signes de sécurité de premier niveau, qu'ils puissent les reconnaitre.

CC 6.3. Le risque de détournement de chèques ou de chéquiers dans les circuits de distribution ou de transport, pouvant notamment se concrétiser par une fraude de type faux (vol/perte) ou falsification.

- La longueur du délai d'acheminement des formules est le principal critère pour déterminer les seuils d'alerte qui seraient déclenchés si le client indique ne pas avoir reçu son chéquier. Néanmoins, si le délai est le principal critère, celui-ci peut être variable selon les territoires et selon les périodes (par exemple, un nombre important de réclamations sur une zone géographique ou à une certaine période de l'année). Il s'agit ainsi d'engager les établissements dans une approche active de mise en opposition des chéquiers récemment envoyés, non reçus par le client, dont ils auraient perdu la trace.
- En pratique, **les procédures d'acheminement qui** « mettent notamment en œuvre des moyens de protection, de surveillance et d'alerte qui répondent à la sensibilité des actifs acheminés » peuvent concerner l'actif lui-même (formules prémarquées, chèques, vignettes, supports de reproduction…), le mode de conditionnement, le contenant, l'environnement, les méthodes de traçabilité, etc.

- Une étude sur les risques liés à la transmission des chéquiers est proposée en complément à la notice. Elle constitue un outil de suivi des risques utilisable, le cas échéant, par chaque établissement dans le cadre de son évaluation de la sécurité.

CC 6.4. : Le risque de rejeu, c'est-à-dire de réutilisation d'un chèque déjà encaissé, qui constitue une des catégories de fraude retenues dans la déclaration statistique de fraude à l'IEOM.

critère b)

- la procédure vise à s'assurer que la destruction est légitime (respect des délais de conservation) et effective (par exemple : engagement contractuel avec le prestataire, clause de responsabilité du prestataire en cas de détournement de vignettes à détruire, traçabilité des lots envoyés à la destruction, présence d'un représentant de l'établissement au moment de la destruction, procès-verbal de destruction…).

critère d)

- il porte sur le risque particulier que présente une vignette pendant sa durée de validité, soit généralement 1 an et 8 jours. Il s'agit, pendant cette période, d'être en mesure d'attester qu'une vignette a bien été détruite, et non d'interpréter son absence après la période des 60 jours calendaires de conservation obligatoire comme une preuve suffisante de sa destruction.

Objectif 7 - Sécurité des environnements des opérations

Cet objectif vise à couvrir les risques inhérents aux environnements physique et logique utilisés par l'établissement déclarant et ses sous-traitants pour la gestion des chèques. Ces risques peuvent notamment se matérialiser sous la forme de cas de fraude des différentes catégories retenues dans la typologie utilisée pour la déclaration statistique à l'IEOM de recensement de la fraude au chèque, tant côté émetteur que remettant (falsification, vol ou perte, contrefaçon, détournement ou rejeu).

CC 7.1. : Le risque d'atteinte à la sécurité des systèmes d'information dédiés aux opérations exercées.

critère d)

- Le risque de fraude est particulièrement visé à travers cet objectif. Les données sensibles du tireur pour les données physiques et logiques ont été identifiées comme suit :
  - fichiers de personnalisation : données qui partent chez le « personnalisateur » ;
  - formules : informations imprimées sur le chèque (notamment n° de compte, référence agence, coordonnées du tireur) ;
  - chèque : signature du tireur.

CC 7.2. : Le risque d'atteinte à la sécurité des environnements de production utilisés pour la gestion des chèques.

Il s'agit des locaux au sens très large, c'est-à-dire ceux où sont stockés, même provisoirement (y compris les agences commerciales), des actifs physiques et ceux où il y a accès à des actifs logiques. Le plan de sécurité visé concerne la protection générale des installations. Cet objectif de protection concerne les locaux d'un établissement comme ceux de ses sous-traitants.

critères b) et c) :

- Le plan de sécurité est formalisé, il régit le filtrage des personnes autorisées. Cet objectif de protection concerne les locaux d'un établissement, y compris les agences commerciales, comme ceux de ses sous-traitants.
- En conséquence, la problématique des accès physiques est à nuancer en fonction des locaux concernés et des opérations chèques (volumes et nature) qui y sont traitées.

CC 7.3. : Le risque de dégradation de la qualité lors des opérations de dématérialisation.

Il s'agit de la phase de reproduction, avant l'archivage. Pour les règles générales concernant l'archivage des vignettes, les établissements se reporteront aux « Règles de l'EIC » en vigueur.

critère a) :

- il ne s'agit pas de contrôler toutes les reproductions, mais de prévoir une procédure de vérification, par exemple par sondages.

critère d) :

- des contrôles ponctuels, par exemple par sondages, permettent de vérifier la bonne conservation des éléments archivés ou de détecter les pertes d'intégrité éventuelles. Il ne s'agit pas de contrôles systématiques de la totalité du stock d'archives

CC 7.4. : Le risque d'atteinte à la sécurité des supports logiques des actifs

Les conditions d'archivage (qualité de l'environnement) des éléments physiques, en tant que supports, sont optimisées. Des contrôles ponctuels, par exemple par sondages, dans les locaux de stockage (ex. : détection des éventuelles dégradations liées à l'humidité, présence de parasites...), sur la lisibilité et l'exploitabilité dans le temps des supports peuvent couvrir cet objectif qui vise à anticiper un éventuel incident. L'établissement dispose par ailleurs d'une solution (deuxième copie, archives sous une autre forme...) lui permettant de pallier la perte d'intégrité éventuelle des archives physiques et logiques. La notion d'intégrité est à adapter en fonction des actifs échangés (chèque original, reproductions ou copies).
Les règles de l'archivage/numérisation des vignettes non circulantes ont l'objet d'une communication adhérent n° 2021/0032 du 23 novembre 2021 – EIC – Les règles de l'Échange d'Images Chèques – Archivage/numérisation référence(s) : communication n° 2005218 du 30/06/2005.

Objectif 8 - Dispositif de surveillance des opérations et de prévention de la fraude

Cet objectif vise à assurer la mise en place par l'établissement d'un dispositif de surveillance des opérations visant à identifier et bloquer les tentatives de fraude, à la fois en tant qu'établissement du remettant (considération clé 8.1) et en tant qu'établissement tiré (considération clé 8.2) et du respect des exigences réglementaires (considération clé 8.3). Chaque établissement définit ses propres procédures en matière de vérification de la présence et de la validité des mentions obligatoires ainsi que l'intégrité des mentions portées sur les chèques en fonction du risque.

CC 8.1. : Cet objectif concerne les contrôles de l'établissement du remettant (le cas échéant de l'établissement remettant) sur les chèques remis à l'encaissement

Sur ce chèque, il est attendu que l'établissement du remettant vérifie non seulement la présence des éléments d'identification du chèque mais aussi leur intégrité (absence de falsification) et dans certains cas leur cohérence (ex : cohérence entre le remettant à l'endos et le bénéficiaire désigné sur le chèque). Il est entendu en revanche qu'il n'a pas à vérifier la cohérence de la signature du tireur. L'établissement du remettant dispose de procédures de vérification et de contrôle de ces différents éléments, qui tiennent compte de sa politique de gestion des risques.

critère a) :

- Il s'agit notamment d'identifier les détournements de chèque (chèque encaissé sur un compte différent de celui du bénéficiaire légitime) et les falsifications (chèque régulier intercepté par un fraudeur qui l'altère volontairement par grattage, gommage ou effacement).
- Les procédures de contrôles consistent à se donner les moyens d'une vérification « efficace » selon, par exemple, les modes de remise, le type de clientèle, … Une analyse de risque propre à chaque établissement le conduira, si nécessaire, à retenir et à faire évoluer les méthodes de contrôle qui lui apparaissent les plus adaptées.
- Les informations d'identification du remettant sont principalement : signature, n° de compte, bordereau de remise ou autres (cas des remises de grands remettants). Celles-ci peuvent être différentes suivant les modalités de remise et les organisations des établissements.

critère d) :

- pour la production des documents réglementaires (avis de rejet, attestation de rejet, Certificat de Non-Paiement) et la gestion des motifs de rejets, les établissements se reporteront aux « Règles de l'EIC » en vigueur, ainsi que notamment à la communication adhérents du CFONB n° 2012/068 du 31 mars 2012 (Chèques sans provision – Modalités d'application du décret n°2011-243 du 4 mars 2011 et de l'arrêté du 20 avril 2011) et à la communication adhérents n° 2014/0032 du 17 juillet 2014 relative aux rejets de chèques et documents liés.

CC 8.2. : Cet objectif vise le dispositif de surveillance et de contrôle des chèques par l'établissement tiré.

critère d) :

- les délais de traitement des opérations considérées comme irrégulières ou frauduleuses relatifs aux opérations EIC figurent dans le document « Les règles de l'EIC » en vigueur.
- Il existe des procédures exceptionnelles pour traiter les opérations qui auraient été effectuées hors délai (communications adhérents n° 2002/307 du 21 novembre 2002 (EIC – restitution hors délai des chèques impayés), n° 2004/076 du 12 mars 2004 (règles de bonne conduite en matière de rejet hors délai de chèques), n° 2005/216 du 30 juin 2005 (dispositions relatives aux échanges hors CORE). Pour traiter les opérations spécifiques dénommées opérations non comptables (ONC), il existe la procédure visée à la communication adhérent n° 2021/0042 du 22 décembre 2021 – EIC les règles de l'Échange d'Images Chèques – Utilisation des opérations non comptables.

CC 8.3. : Cet objectif vise les exigences réglementaires lors des opérations d'émission, d'encaissement et de dématérialisation de chèques.

critère a) :

- Ce critère concerne l'image chèque qui est faite à partir du chèque hors les opérations connexes. Ce critère vise le risque de présentation de plusieurs IC à partir d'un même actif chèque, avec ou

sans la même identification d'opération. Ce critère vise plus précisément le fait que l'établissement n'envoie qu'une IC par chèque. Il couvre le risque de doublon.

- Concernant le risque de dématérialisation d'une vignette (chèque déjà dématérialisé), les établissements se reporteront à la communication adhérents n° 2008/011 du 7 janvier 2011 (évolution des règles de l'EIC en matière de contrôle de doublons CMC7). Cet objectif peut être atteint par la mise en œuvre de contrôles, soit :
  - en amont du système de paiement par chèque, afin d'éviter d'y introduire une IC qui correspondrait à la dématérialisation d'une vignette (chèque déjà payé) ;
  - en aval, pour l'ensemble des établissements, afin de s'assurer avant le paiement définitif de l'IC que celle-ci n'a pas déjà été payée.
- Pour les valeurs perdues avant remise par les clients à leur établissement et celles après remise par les clients à leur établissement, les établissements se reporteront respectivement aux communications adhérents n° 2010/190 du 21 juillet 2010 (Règlement interbancaire des valeurs perdues après remise par les clients à leur établissement) et 2005/343 du 21 octobre 2005 (Règlement interbancaire des valeurs perdues après remise par les clients à leur établissement – chèques et effets de commerce).
- Sur le point de l'identification de l'opération, les établissements se reporteront aux Règles de l'EIC en vigueur.

critère b) :

- sur les modalités de circulation des vignettes, les établissements se réfèreront aux « Règles de l'EIC » en vigueur ainsi qu'au règlement intérieur du Centre d'Échanges Physiques des Chèques.

critère c) :

- les délais réglementaires visés sont ceux de l'article R131-32 du code monétaire et financier : « *Le banquier avise la Banque de France des clôtures de comptes autres que celles qui résultent d'un transfert dans son établissement et des oppositions à paiement mentionnées à l'article L. 131-84* ***dans le meilleur délai et au plus tard le premier jour ouvré suivant la clôture du compte ou l'opposition à paiement****. À cette fin, il communique les renseignements prévus au 1° de l'article R. 131-12, ainsi que, s'il en a connaissance, les numéros des formules de chèque volées ou perdues.* ». Cet article est applicable en Nouvelle-Calédonie, en Polynésie française et sur les îles Wallis-et-Futuna respectivement en vertu des articles R. 732-10, R. 733-10 et R. 734-10.
- les délais de déclaration aux fichiers FCC et FNCI de la Banque de France sont précisés aux articles R. 131-26 et R. 131-31 du Code monétaire et financier. Ces articles sont applicables en Nouvelle-Calédonie sur la base de l'article R. 732-9, en Polynésie française par l'article R. 733-9 et sur les iles de Wallis-et-Futuna par l'article R. 734-9. Les modalités de déclaration au FNCI sont précisées dans une procédure de la Banque de France de janvier 2019. Pour le cas particulier des faux chèques, le remettant pourra se reporter à la communication adhérents n° 2022/0014 du 31 mai 2022 (Procédure de déclaration des faux chèques au fichier national des chèques irréguliers (FNCI) de la Banque de France).

Objectif 9 - Sensibilisation des clients aux règles de sécurité

Cet objectif vise à assurer un niveau d'information suffisant aux utilisateurs permettant à ces derniers de contribuer à la sécurité des opérations les concernant, notamment au titre de la détention de formules de chèques et de chèques émis (considération clé 9.1), des risques de fraude possibles liés à l'acceptation d'un chèque comme moyen de règlement (considération clé 9.2), du suivi des opérations réalisées avec l'établissement (imputation des opérations sur le compte, renouvellement des formules de chèques et de mise à disposition (considération clé 9.3) ou de l'utilisation de dispositifs de rédaction automatique de chèques (considération clé 9.4).

CC 9.1 : Sensibilisation des clients tireurs

critère a) :

- pour les recommandations sur l'utilisation et la rédaction de chèques, les établissements se reporteront notamment à la communication adhérents n° 2022/0018 du 23 juin 2022 (recommandations sur l'utilisation et la réd (action de chèques).

critères a) et b) :

- il s'agit bien d'une formalisation écrite, quel que soit le support (page web, chéquiers, applications mobiles…) et quelle que soit la clientèle.

CC 9.2. : Sensibilisation des clients remettants

Il est attendu que l'établissement mette à la disposition de ses clients accepteurs de chèque des outils de contrôle de la régularité des chèques (par exemple sur applications mobiles sur automates de remises de chèques avec interrogation potentielle du FNCI). S'il ne met pas à disposition ni ne développe de tels outils, il communique « *au minimum* » sur des services disponibles sur le marché (ex: Vérifiance, autres outils de vérification des chèques avant acceptation). Via le terme « *intérêt* », il est attendu que l'établissement appelle l'attention de son client sur les capacités de ces outils en matière de prévention contre la fraude au chèque, mais aussi sur les précautions à prendre (par exemple, une réponse « verte » dans Vérifiance ne prémunit pas totalement contre le risque de fraude). Via le terme « *éligible* », l'établissement comprendra qu'il n'y a pas d'exigence à communiquer auprès des particuliers sur l'outil Vérifiance qui ne leur est pas aujourd'hui accessible.

critère b) :

- s'agissant de l'encaissement de chèques pour le compte de tiers, l'IEOM effectue des communications (y compris vidéos) sur lesquelles la profession pourra s'appuyer ou relayer.

CC 9.4. : Sécurité des dispositifs de remplissage automatique de chèques

critère a) :

- pour l'information de leurs clients, les établissements se reporteront à la communication adhérents n° 1998/215 du 23 juin 1998 (rédaction automatique des chèques au point de vente).

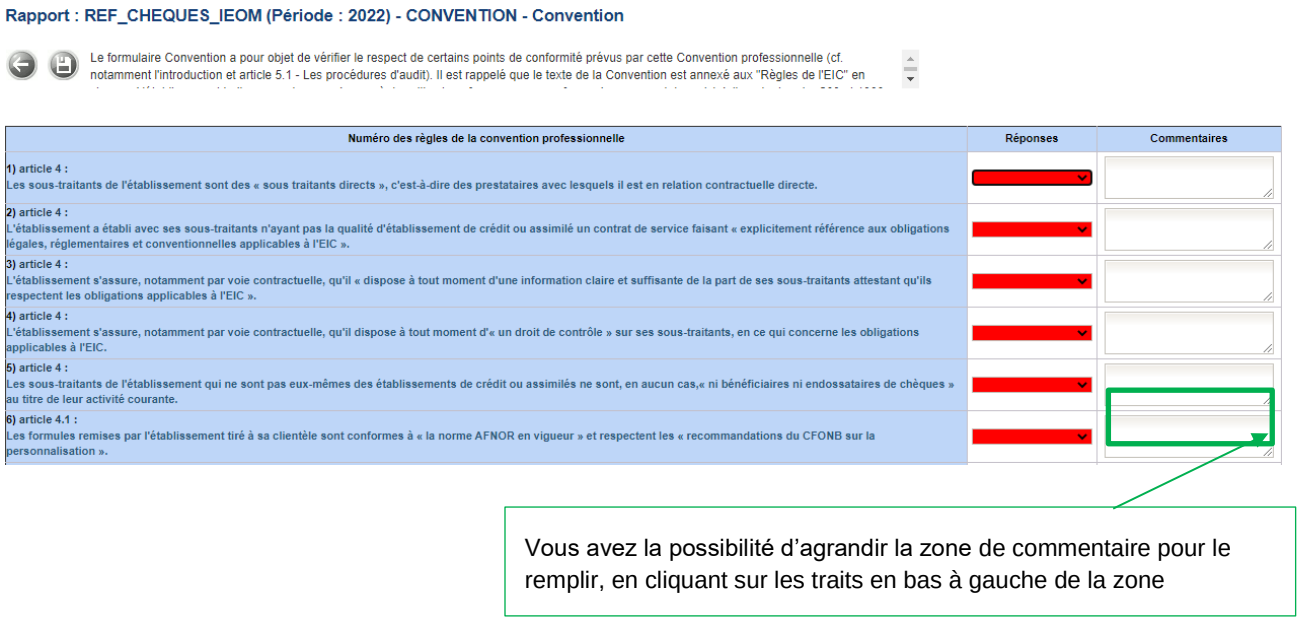
De façon générale, le déclarant pourra se reporter à la communication adhérents n° 2022/0015 du 31 mai 2022 – Chèque bancaire, Références législatives et réglementaires et recommandations de la Profession qui est un recueil des principales références existantes sur le chèque bancaire en euros payable en France, qu'elles soient de type réglementaire ou sous forme de recommandations.

4.5. Section 3 : Formulaire Respect de la Convention professionnelle EIC

4.5.1. Modalités de déclaration

Le formulaire Respect de la Convention professionnelle EIC a pour objet de vérifier le respect, par les établissements, de certains points de conformité prévus par cette Convention Professionnelle. Il est rappelé que le texte de la Convention est annexé aux "Règles de l'EIC" en vigueur et disponible sur l'intranet du CFONB.

Ce formulaire présente certains des points de conformité à la convention professionnelle.



Description des contraintes et contrôles de la section

- Pour chacun de ces points, le déclarant devra répondre « CONFORME » ou « NON CONFORME ».
- Un commentaire est obligatoire lorsque la réponse choisie est « NON CONFORME ». Le commentaire saisi doit contenir entre 200 et 1 000 caractères.
    - Si le nombre de caractères est inférieur à 200 caractères, le message suivant apparaît : « Le commentaire saisi doit contenir au moins 200 caractères »
    - Si le nombre de caractères est supérieur à 1 000 caractères, le message suivant apparaît : « Le commentaire saisi ne doit pas contenir plus de 1 000 caractères »

4.5.2. Points de conformité de la convention professionnelle couverts par le formulaire

La liste des points de conformité prévus par la convention professionnelle est rappelée pour mémoire dans le tableau ci-après :

N°	Art	Obligation
1	4	Les sous-traitants de l'établissement sont des « sous-traitants directs », c'est-à-dire des prestataires avec lesquels il est en relation contractuelle directe
2	4	L'établissement a établi avec ses sous-traitants n'ayant pas la qualité d'établissement de crédit ou assimilé un contrat de service faisant « explicitement référence aux obligations légales, réglementaires et conventionnelles applicables à l'EIC »

N°	Art	Obligation
3	4	L'établissement s'assure, notamment par voie contractuelle qu'il « dispose à tout moment d'une information claire et suffisante de la part de ses sous-traitants attestant qu'ils respectent les obligations applicables à l'EIC »
4	4	L'établissement s'assure, notamment par voie contractuelle, qu'il dispose à tout moment d'« un droit de contrôle » sur ses sous-traitants, en ce qui concerne les obligations applicables à l'EIC
5	4	Les sous-traitants de l'établissement qui ne sont pas eux-mêmes des établissements de crédit ou assimilés ne sont, en aucun cas, « ni bénéficiaires ni endossataires de chèques » au titre de leur activité courante
6	4.1	Les formules remises par l'établissement tiré à sa clientèle sont conformes à « la norme AFNOR en vigueur » et respectent les « recommandations du CFONB sur la personnalisation »
7	4.1	L'établissement tiré s'assure que les lettres-chèques éditées par ses clients sont conformes à « la norme AFNOR en vigueur » et respectent « les recommandations du CFONB sur la personnalisation »
8	4.1	L'établissement tiré s'assure que les lettres-chèques éditées par ses clients « respectent les règles du CFONB spécifiques à l'établissement de ces formules »
9	4.2.2	L'établissement remettant « contrôle le caractère magnétique ou non de la ligne CMC7 de la vignette »
10	4.2.2	L'établissement remettant établit « un document de rejet en cas de retour impayé de l'image-chèque d'une vignette qu'il a conservée pour le compte de l'établissement tiré »
11	4.2.2	Au travers de l'avis de rejet, l'établissement remettant porte à la connaissance du bénéficiaire du chèque « les irrégularités décelées » lors des contrôles effectués en cas de retour impayé de l'IC
12	4.2.2	L'établissement remettant porte à la connaissance de l'établissement tiré, « dans les meilleurs délais », les irrégularités décelées lors des contrôles effectués en cas de retour impayé de l'IC, « si le motif de rejet est l'absence ou l'insuffisance de provision »
13	4.3	L'établissement qui n'est pas établissement remettant s'interdit de procéder à la dématérialisation de chèques
14	4.3.1	L'établissement remettant constitue des images-chèques comprenant les éléments définis dans les règles EIC du CFONB
15	4.3.1	L'établissement remettant ne constitue une image-chèque que s'il satisfait « impérativement » à la condition prévoyant la « disposition matérielle et préalable du chèque » correspondant
16	4.3.1	L'établissement remettant constitue l'image chèque à partir de « l'exploitation automatique ou manuelle des informations figurant sur la vignette, le montant seul pouvant être repris d'un fichier fourni par ailleurs par l'un quelconque des intervenants antérieurs, remettant compris »
17	4.4	L'établissement remettant procède à l'échange des vignettes circulantes correspondant aux images-chèques qu'il a émises « dans le respect des délais définis par le CFONB »
18	4.5.1	L'établissement remettant qui a constitué l'image-chèque assure, « sans substitution » possible, « l'archivage des vignettes définies comme non circulantes » pour le compte de l'établissement tiré
19	4.5.1	L'établissement remettant ne délègue « en aucun cas » l'archivage de la vignette définie comme non circulante « au bénéficiaire ou à l'endossataire du chèque si celui-ci n'est pas par ailleurs établissement remettant »
20	4.5.2	L'établissement remettant archive, « durant 10 ans », les vignettes non circulantes ou leurs copies
21	4.5.2	L'établissement remettant respecte les règles et normes définies par le CFONB pour l'archivage des copies en matière de « fidélité et de durabilité des reproductions, conformément à l'article 1348 du Code Civil »

N°	Art	Obligation
22	4.5.2	L'établissement remettant respecte les règles et normes définies par le CFONB pour l'archivage des vignettes non circulantes ou de leur copie en matière de « sécurité physique de la conservation »
23	4.5.2	L'établissement remettant respecte les règles et normes définies par le CFONB pour l'archivage des vignettes non circulantes ou de leur copie en matière de production de la copie « sur un support lisible et exploitable par le destinataire »
24	4.5.2	L'établissement remettant doit pouvoir fournir l'original de la vignette non circulante archivée pendant « 60 jours calendaires à compter de la date d'échange dans le système de l'image-chèque correspondante »
25	4.5.2	L'établissement remettant doit pouvoir fournir durant 10 ans « la copie recto verso du chèque, même si le chèque a été restitué au client remettant en cas d'impayé »
26	4.5.2	L'établissement remettant s'est mis en situation de pouvoir identifier « une vignette à partir de sa référence d'archivage » durant les 10 ans de la période d'archivage
27	4.6.1	L'établissement remettant répond à la demande de transmission de « l'original ou de la copie du chèque » émanant de l'établissement tiré, dans le respect « du délai maximum de réponse à ce type de requête » arrêté par le CFONB
28	4.7.1	L'établissement tiré établit en cas de non-paiement « l'avis de rejet, l'attestation de rejet ou le certificat de non-paiement » pour les vignettes qui sont en sa possession
29	4.7.2.2	Pour les chèques définis comme non circulants, l'établissement remettant « procède à un examen formel du titre permettant d'assurer que l'absence de provision constitue bien le motif déterminant du rejet », lorsque celui-ci lui a été notifié par l'établissement tiré dans le rejet d'image-chèque correspondant
30	4.7.2.2	Pour les chèques définis comme non circulants, l'établissement remettant apprécie, en se fondant sur la date d'émission du titre, « si un chèque impayé a ou non été émis en violation d'une interdiction bancaire ou judiciaire », lorsque celle-ci lui a été notifiée par l'établissement tiré dans le rejet d'image-chèque correspondant
31	4.7.2.2	Lorsqu'après vérification par l'établissement remettant, un chèque s'avère avoir été émis en violation d'une interdiction bancaire ou judiciaire, « cette information est portée sur l'attestation de rejet et portée sans délai à la connaissance de l'établissement tiré »

5. COMPLÉMENTS À LA NOTICE

5.1. Risques identifiés en matière de transmission des moyens de paiement

5.1.1. Glossaire

Sur-contenant = Lors de l'expédition, tout conditionnement visible au moment de la prise en charge par le transporteur. Il peut contenir plusieurs contenants dans lesquels se trouvent les carnets de chèques. Le « sur-contenant » peut être un carton, une palette, un sac, un chariot…

Intégrité du sur-contenant = le contenu ne peut être atteint.

Défaut application procédure = concerne à la fois le transport du colis, ou les documents liés (bordereau par exemple).

Non-prise en compte du caractère particulier du pli = mauvaise détection de la qualité du pli.

Remise du pli au destinataire (étape du processus n° 4) = L'indicateur du risque sera différent en fonction de la situation : remise en mains propres du pli ou dépôt du pli.

Dépôt en boîte à lettres = La sécurisation de la boîte à lettres fait partie de l'environnement, elle est donc considérée comme hors périmètre.

Mise en place d'une procédure = Dès lors qu'une procédure est en place, elle doit faire l'objet de contrôles selon une périodicité définie par l'établissement.

Emballage = De façon générale, quelle que soit l'étape du traitement, le moyen de paiement ne doit pas apparaître. À titre d'exemple, carton, enveloppe utilisée pour le transport du moyen de paiement.

Sécurité du transport = À chaque étape, la sécurité du moyen de transport utilisée doit être assurée.

Réactivité = À chaque étape, une réactivité forte est attendue dès lors qu'un incident est relevé.

Plis Non Distribuables ou PND = « NPAI » (n'habite pas à l'adresse indiquée).

5.1.2. Prise en charge du « sur-contenant » par le transporteur

Lieu : chez le prestataire ayant fabriqué les chéquiers

Risque identifié	Préconisations	Exemples de couverture des besoins*
Perte, Vol, Détournement de chéquier(s)		
1. Intégrité du « sur-contenant »	prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu	• double SAS avec empêchement d'ouverture simultanée des deux portes • Films plastiques autour du « sur-contenant » • Chariot grillagé - fermé
2. Erreur liée à la manipulation	2. à 5. Mettre en place une procédure de prise en charge du « sur-contenant » couvrant l'identification du « sur-contenant », du prestataire ou des éléments permettant le suivi du « sur-contenant »	2. à 5 : • Badges d'accès du transporteur • Reconnaissance contradictoire et prise en charge • Présence d'un bordereau d'identification du « sur-contenant » • Identification individuelle du "sur-contenant" (étiquetage - code à barres, etc.) • Flashage du « sur-contenant » remis par le personnalisateur
3. Non-prise en compte du caractère particulier des plis contenus dans le « sur-contenant »		
4. Perte de l'identifiant, perte de la traçabilité		
5. Erreur de prise en charge du « sur-contenant »		

* non limitatifs - d'autres solutions peuvent être proposées

Traitement du « sur-contenant »

Fonctions concernées :

- Prise en charge,
- Ouverture,
- Séparation des colis individuels

Lieu : dans la structure qui reçoit les « sur-contenants », les ouvre et assure la répartition des colis

Risque identifié	**Préconisations**	**Exemples de couverture des besoins***
Perte, Vol, Détournement de chéquier(s)		
1. Perte de l'intégrité du « sur-contenant »	• Prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu • Prévoir une procédure de prise en charge du « sur-contenant » à l'arrivée	• Traitement assuré dans un local spécifique • Accès limités • Reconnaissance contradictoire et prise en charge • Identification individuelle du « sur-contenant » (étiquetage - code à barres, etc.) • Flashage du « sur-contenant » à l'arrivée • Établissement d'un état des anomalies • Alerte en cas de problème
2. Perte de l'intégrité du colis lors de l'ouverture du « sur-contenant »	• Mettre en place une procédure d'ouverture du « sur-contenant »	• Badges d'accès des manipulateurs • Présence d'un bordereau d'identification du contenu du « sur-contenant » • Reconnaissance contradictoire et prise en charge • Établissement d'un état des anomalies • Alerte en cas de problème
3. Erreur liée à la manipulation	3. à 6. • Mettre en place une procédure de séparation des colis, couvrant l'identification des colis, du prestataire ou des éléments permettant le suivi des colis	3. à 6 : • Identification individuelle de chaque colis (étiquetage - code à barres, etc.) • Flashage de chaque colis au départ • Établissement d'un état des anomalies • Alerte en cas de problème.
4. Non-prise en compte du caractère particulier des plis contenus dans le colis		
5. Perte de l'identifiant, perte de la traçabilité		
6. Erreur de réacheminement des colis		

* non limitatifs - d'autres solutions peuvent être proposées

Traitement et envoi du colis par la structure qui trie et expédie les plis

Lieu : Service du prestataire (transporteur ou banque)

Risque identifié	Préconisations	Exemples de couverture des besoins*
Perte, Vol, Détournement de chéquier(s)		
1. Perte de l'intégrité du colis	• Prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu • Prévoir une procédure de prise en charge du colis à l'arrivée	• Traitement assuré dans un local spécifique • Accès limités • Reconnaissance contradictoire et prise en charge • Identification individuelle du colis (étiquetage - code à barres, etc.) • Flashage du colis à l'arrivée • Établissement d'un état des anomalies • Alerte en cas de problème
2. Perte de l'intégrité du pli lors de l'ouverture du colis	• Mettre en place une procédure d'ouverture du colis	• Intervention par collaborateur(s) identifié(s) • Reconnaissance contradictoire et prise en charge • Présence d'un bordereau d'identification du contenu du colis (les plis) • Identification individuelle de chaque pli (étiquetage - code à barres, etc.) • Flashage du pli à l'arrivée • Établissement d'un état des anomalies • Alerte en cas de problème

3. Erreur liée à la manipulation
4. Perte de l'identifiant, perte de la traçabilité
5. Erreur de réacheminement des plis
	3. à 5.
	• Mettre en place une procédure de :
	  ○ prise en charge des plis, couvrant l'identification des plis, du prestataire ou des éléments permettant le suivi des plis
	  ○ conservation des plis dans l'attente de leur remise au destinataire ou au prestataire avant délivrance au destinataire
		3. à 5 :
		• Identification individuelle des plis (étiquetage - code à barres, etc.)
		• Flashage de chaque pli au départ
		• Établissement d'un état des anomalies
		• Alerte en cas de problème.

* non limitatifs - d'autres solutions peuvent être proposées

Remise du pli au destinataire (client)

Risque identifié	Préconisations	Exemples de couverture des besoins*
Perte, Vol, Détournement de chéquier(s)		
1. Perte de l'intégrité du pli	• Prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu • Prévoir une procédure de prise en charge à l'arrivée du pli	• Transport dans des conditions adaptées « sous surveillance » • Reconnaissance contradictoire et prise en charge • Identification particulière du pli (étiquetage - code à barres, etc.) • Flashage du pli • Établissement d'un état des anomalies • Alerte en cas de problème
2. Défaut d'application de la procédure, erreurs liées à la manipulation	2. à 5. • Mettre en place une procédure de remise du pli et de réacheminement du pli en cas de non remise, couvrant l'identification du pli, du prestataire ou des éléments permettant le suivi du pli	2 à 5 • Intervention par collaborateur(s) identifié(s) • Reconnaissance contradictoire et prise en charge • Présence d'un bordereau d'identification du pli • Identification individuelle du pli (étiquetage - code à barres, etc.) • Identification du destinataire ou délivrance à un mandataire habilité • Flashage du pli à l'arrivée (remise ou retour non distribué) • Établissement d'un état des anomalies • Alerte en cas de problème
3. Non prise en compte du caractère particulier du pli (notamment conservation/conditions de remise)		
4. Perte de l'identifiant, perte de la traçabilité		
5. Erreur de réacheminement du pli		

* non limitatifs - d'autres solutions peuvent être proposées

Non-remise du pli au destinataire lors de l'acheminement ou du réacheminement

Cas d'absence, d'impossibilité de remise au lieu de dépôt prévu, de plis non-distribuables (PND), etc.

Risque identifié	Préconisations	Exemples de couverture des besoins*
Perte, Vol, Détournement de chéquier(s)		
1. Perte de l'intégrité du pli	• Prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu • Prévoir une procédure si le pli est ouvert	• Sécurisation lors du transport retour puis à l'arrivée – conditions adaptées- • Reconnaissance contradictoire et prise en charge • Identification particulière du pli (étiquetage - code à barres, etc.) • Flashage du pli • Établissement d'un état des anomalies • Alerte en cas de problème
2. Défaut d'application de la procédure, erreurs liées à la manipulation	2. à 4. • Mettre en place une procédure de ○ conservation du pli en attente d'être retourné ○ prise en charge du pli couvrant l'identification du pli, du prestataire ou des éléments permettant le suivi du pli	2 à 4 • Intervention par collaborateur(s) identifié(s) • Reconnaissance contradictoire et prise en charge • Présence d'un bordereau d'identification du pli • Identification individuelle du pli (étiquetage - code à barres, etc.) • Conservation dans un espace spécifique • Flashage du pli à l'arrivée (remise ou retour non distribué) • Établissement d'un état des anomalies • Alerte en cas de problème
3. Non prise en compte du caractère particulier du pli (notamment lors de la conservation)		
4. Perte de l'identifiant, perte de la traçabilité		

* non limitatifs - d'autres solutions peuvent être proposées

Retour du pli vers l'expéditeur (personnalisateur ou tout autre site) ou destruction

Risque identifié	Préconisations	Exemples de couverture des besoins*
Perte, Vol, Détournement de chéquier(s)		
1. Perte de l'intégrité du pli	• Prévoir tout moyen/procédé permettant d'éviter un accès au contenu ou sa dispersion et/ou qui permette la détection d'une éventuelle atteinte au contenu • Prévoir une procédure si le pli est ouvert	• Sécurisation de l'emballage du pli • Reconnaissance contradictoire et prise en charge • Identification particulière du pli (étiquetage - code à barres, etc.) • Flashage du pli • Établissement d'un état des anomalies • Alerte en cas de problème
2. Défaut d'application de la procédure, erreurs liées à la manipulation 3. Perte de l'identifiant, perte de la traçabilité 4. Erreur de réacheminement des plis	2. à 4. • Mettre en place une procédure couvrant l'identification du pli, du prestataire ou des éléments permettant le suivi du pli ○ au retour du pli vers l'expéditeur ou une autre structure spécialisée ○ à la destruction du pli	2 à 4 • Intervention par collaborateur(s) identifié(s) • Reconnaissance contradictoire et prise en charge • Présence d'un bordereau d'identification du pli • Identification particulière du pli (étiquetage - code à barres, etc.) • Conservation dans un espace spécifique • Flashage du pli à l'arrivée (retour ou en voie d'être détruit) • Local sécurisé (si destruction) • Procès-verbal de destruction • Information du donneur d'ordre (si destruction) • Établissement d'un état des anomalies • Alerte en cas de problème

* non limitatifs - d'autres solutions peuvent être proposées

5.2. Table de correspondance entre objectifs des RSC 2005/2016/2022

Les établissements pourront retrouver dans le tableau de correspondance ci-dessous les jonctions entre les objectifs de sécurité définis dans les différentes versions du Référentiel de sécurité du chèque (RSC) depuis sa première version en 2005.

Tableau de correspondance RSC