Audits de contrôle annuels REMPARTS

Modalités de réalisation et contrôles attendus

Version 1.0 (janvier 2022)

1 Introduction

Lors du club utilisateurs REMPARTS du 1er octobre 2021, les participants ont demandé à CB de préciser la portée de l'audit de contrôle annuel auquel sont soumises les sociétés labélisées. Pour rappel, les grandes lignes de cet audit sont définies comme suit dans le document de cadre général REMPARTS (chapitre 3.3) :

> *Les sociétés labélisées devront se soumettre à un audit de contrôle annuel, dont la réalisation conditionne le maintien de la Labélisation REMPARTS, et dont le rapport sera rédigé par un auditeur habilité REMPARTS et validé par CB.*
>
> *Ce rapport devra attester :*
>
> - *Que les plans d'actions établis lors de l'audit initial et lors des tests d'intrusion annuels sont bien suivis,*
> - *Qu'aucun changement dans l'organisation de la société ou dans ses activités n'est susceptible d'avoir remis en cause sa conformité aux exigences REMPARTS applicables,*
> - *Que les contrôles périodiques mis en œuvre pour répondre aux exigences qui s'appliquent à leurs activités sont bien effectués.*

Cette note a pour objet de préciser la liste des contrôles attendus, les prérequis et les conditions de réalisation de ces audits.

2 Références

La présente note fait référence aux exigences du référentiel REMPARTS (DPE-ESS-REF-2016-006) en version 2.0, daté d'avril 2019 et consultable sur le portail REMPARTS.

Cette note pourra être amenée à évoluer lorsqu'une mise à jour de ce référentiel sera publiée. Cependant, les modalités applicables aux sociétés labélisées resteront stables pour toute la durée de leur labélisation.

Toutes les exigences pointées par cette note font partie du tronc commun. Elles sont donc applicables à l'ensemble des acteurs labélisés. Les références à ces exigences sont toutes de la forme EXI_TC_XX, où XX correspond au numéro de l'exigence.

3 Conditions de réalisation des audits de contrôle

3.1 Modalités de réalisation des audits de contrôle

Les audits de contrôle doivent être effectués par l'une des sociétés habilitées par PayCert pour les audits de labélisation REMPARTS.

Sauf cas exceptionnel validé préalablement avec CB et la société labélisée, ces audits ne nécessitent pas de déplacement sur site et peuvent donc être réalisés à distance. La charge nécessaire à l'exécution de ces audits est laissée à l'appréciation des sociétés d'audit et des sociétés labélisées contractualisant avec elles. Toutefois, sauf cas exceptionnel dûment justifié et validé avec CB, elle ne devrait jamais excéder 3 jours.

3.2 Période de réalisation des audits de contrôle

Les sociétés labélisées sont soumises à deux audits de contrôle :

- Le premier audit doit avoir lieu au plus tôt 11 mois après la prononciation de la labélisation, et avant que 13 mois complets ne se soient écoulés
- Le second audit doit avoir lieu au plus tôt 23 mois après la prononciation de la labélisation, et avant que 25 mois complets ne se soient écoulés.

À titre d'exemple, une société labélisée en avril 2022 devra fournir à CB son premier rapport de contrôle au plus tôt en mars 2023, et au plus tard fin mai 2023. De même, elle devra fournir à CB son second rapport de contrôle au plus tôt en mars 2024, et au plus tard en mai 2024.

La bonne réalisation de ces audits conditionne le maintien de la labélisation REMPARTS.

3.3 Rapports d'audit de contrôle

La structure du rapport n'est pas figée, mais elle doit être formalisée par la société d'audit. Sauf cas de force majeure, les deux rapports de contrôle doivent partager la même structure et être aisément comparables.

Le document doit préciser la période d'audit, la charge associée, l'ensemble des livrables fournis pour l'audit, et l'échantillonnage effectué, le cas échéant.

Les rapports d'audit de contrôle sont validés directement par CB, sans frais associés, et n'impliquent pas de certification. Ils doivent être envoyés à l'adresse labelisation@cartes-bancaires.com dans les délais précisés dans cette note. Ils peuvent être transmis soit par la société d'audit directement, soit par la société labélisée si elle le souhaite.

Dans tous les cas, la société labélisée et la société d'audit doivent être informées de cet envoi.

4 Liste des contrôles attendus

4.1 Suivi des mises à jour documentaires

Plusieurs processus de sécurité s'appuient sur des procédures qui sont susceptibles d'être mises à jour régulièrement. Lors de l'audit de contrôle annuel, la société labélisée doit indiquer à la société d'audit quels documents et quelles procédures ont fait l'objet d'une telle mise à jour, et lui donner la possibilité de les consulter.

Au minimum, les éléments suivants doivent être considérés :

- Le document formalisant l'appréciation des risques (EXI_TC_2)
- La politique de sécurité (EXI_TC_3)
- La charte de sécurité (EXI_TC_5)
- La cartographie du réseau (EXI_TC_40)

Si aucune mise à jour de document ou de procédure n'a eu lieu dans l'année précédant l'audit de contrôle, cette absence de mise à jour doit être consignée dans le rapport de contrôle.

4.2 Suivi de l'exécution des contrôles périodiques

Afin que la société réalisant l'audit de contrôle puisse évaluer, par échantillonnage, que les contrôles périodiques requis sont bien réalisés, la société labélisée doit préparer et fournir, en amont de l'audit de contrôle les éléments suivants :

- Le procès-verbal de la dernière séance de sensibilisation du personnel (EXI_TC_6)
- Les procès-verbaux des 4 dernières revues des droits d'accès physiques et des 2 derniers contrôles de besoins (EXI_TC_15)
- Le procès-verbal de contrôle annuel des installations de sécurité physique (EXI_TC_17)
- Les procès-verbaux des 4 derniers contrôles des droits d'accès logiques (EXI_TC_20, EXI_TC_27)
- Le procès-verbal du dernier contrôle des configurations des équipements réseaux (EXI_TC_26)
- Les procès-verbaux des 4 derniers contrôles des mises à jour logicielles non critiques, et des 12 derniers contrôles de mises à jour logicielles critiques (EXI_TC_28, EXI_TC_30)
- Les synthèses et plans d'action des rapports de test d'intrusion interne et externes (EXI_TC_46)
- Les 12 derniers compte-rendu de contrôle permanent, ainsi que les compte-rendu de contrôle périodique pour l'année écoulée (EXI_TC_47)
- Les rapports d'audit de sous-traitance de l'année écoulée (EXI_TC_51)
- La liste des incidents de sécurité identifiés dans les 12 derniers mois (EXI_TC_53)

Lorsqu'un procès-verbal ne peut pas être fourni à la société réalisant l'audit, tout élément de preuve de nature à pallier l'absence de ce document peut être demandé par celle-ci afin d'établir les constats nécessaires.

4.3 Suivi des plans d'action établis

Le statut de toutes les actions en attente de résolution au moment de la prononciation de la Labélisation doit être documenté par la société d'audit dans chaque rapport de contrôle.

En complément, les éventuels plans d'actions établis lors des campagnes annuelles de tests d'intrusion internes et externes doivent être intégrés à ce suivi, et doivent donc figurer dans les rapports de contrôle.

4.4 Suivi des changements organisationnels

Tout changement de nature à modifier l'organisation de la société labélisée doit être documenté, et son impact doit être évalué par la société réalisant l'audit. Ces changements incluent notamment :

- Les évolutions dans les activités opérées par la société labélisée, dès lors qu'elles sont susceptibles d'avoir un impact sur le périmètre ou les contraintes liées à la labélisation REMPARTS.
- Les mouvements de personnel encadrant en lien avec les activités monétiques.
- Les travaux ayant eu un impact sur la sécurité physique des locaux ou sur l'organisation des activités couvertes par la labélisation REMPARTS.
- La mise en place de nouveaux outils informatiques sur lesquels s'appuient des processus couverts par la labélisation REMPARTS.

4.5 Suivi des activités sensibles

La société d'audit peut, lorsqu'elle le juge pertinent, compléter les contrôles décrits dans cette note par des contrôles supplémentaires ciblant les activités sensibles de la société labélisée. Ces contrôles additionnels devront être décrits dans le rapport soumis à CB.

Note rédigée par : Emmanuel le Chevoir
Date de publication : 31 janvier 2022
Référence de la note : DPE-ESS-NTE-2022-002
Révision : 1.0
Classification : Diffusion publique