INFORMATIONS SUPPLÉMENTAIRES

PCI DSS v4.x : Directives Relatives Aux Mesures de Sécurité Compensatoires et à l'Approche Personnalisée

Version : 1.0
Date : Juin 2026
Auteur : PCI Security Standards Council

Modifications Apportées au Document

Date	Version	Description
Juin 2026	1.0	Version initiale

REMERCIEMENTS: La version anglaise de ce document, telle que mise à disposition sur le site Internet du PCI SSC, à toutes fins, est considérée comme la version officielle de ces documents et, dans la mesure où il existe des ambiguïtés ou des incohérences entre la rédaction de ce texte et du texte anglais, la version anglaise disponible à l'endroit mentionné prévaudra.

Contenu

Aperçu

Le Payment Card Industry Data Security Standard (PCI DSS) favorise la flexibilité dans la manière d'atteindre les objectifs de sécurité. La version 4.x du PCI DSS prévoit deux approches pour l'implémentation et la validation des contrôles PCI DSS : l'approche définie et l'approche personnalisée. Ces deux approches diffèrent par leur objectif, leurs éléments, leur documentation et leur validation.

Le présent document présente chacune de ces approches et :

- Aborde le rôle des entités évaluées
- Aborde le rôle des évaluateurs associés, et
- Fournit de la documentation relative à ces approches ainsi que des réponses aux questions fréquemment posées.

À l'intention des entités évaluées, ce document comprend des exemples complétés de :

- Fiche D'Identification des Mesures Compensatoires
- Une Matrice des Contrôles pour une Approche Personnalisée, et
- Une Analyse Ciblée des Risques pour l'Approche Personnalisée.

À l'intention des évaluateurs, ce document comprend un exemple complété de Rapport de Conformité — Modèle de l'Annexe E pour l'Approche Personnalisée.

Public et Objectif

Le présent document s'adresse à toutes les entités qui développent, exploitent, gèrent ou évaluent des mesures de sécurité compensatoires ou une approche personnalisée. Cela inclut les évaluateurs qui réalisent des évaluations PCI DSS, ainsi que les entités qui y sont soumises.

L'objectif de ce document est de fournir des conseils pratiques afin de favoriser une utilisation cohérente des mesures de sécurité compensatoires et de l'approche personnalisée.

Le PCI Security Standards Council (PCI SSC) n'est pas chargé de faire respecter la conformité ni de déterminer si une mise en œuvre particulière est conforme. Les entités doivent collaborer avec l'organisme ou les organismes chargés de gérer leur programme de conformité, tels qu'un acquéreur (banque commerciale), une marque de paiement ou toute autre entité, afin de comprendre les responsabilités de l'entité en matière de validation et de rapports de conformité.

Les directives contenues dans le présent document ne viennent ni compléter, ni étendre, ni remplacer, ni prévaloir sur les exigences du PCI DSS ou de toute autre standard du PCI SSC. Au moment de la publication, la version actuelle de la norme PCI DSS est la v4.0.1 ; toutefois, les principes généraux et les pratiques présentés ici peuvent également s'appliquer aux versions futures.

Options pour Implémenter et Valider les Contrôles PCI DSS v4.x

PCI DSS v4.x propose deux façons pour une entité d'implémenter et de valider les exigences PCI DSS – l'approche définie et l'approche personnalisée.

L'approche définie est la méthode traditionnelle pour implémenter et valider les contrôles PCI DSS, en place depuis la première version de PCI DSS. **Les mesures de sécurité compensatoires sont une option dans l'approche définie** pour les entités qui ont une contrainte technique ou commerciale légitime et documentée les empêchant de satisfaire l'exigence de l'approche définie telle qu'énoncée. Les mesures de sécurité compensatoires sont souvent utilisées dans des situations où un système ou un processus existant ne peut pas être mis à jour pour répondre à l'exigence.

L'approche personnalisée se concentre sur l'objectif de sécurité de chaque exigence PCI DSS (le cas échéant), permettant aux entités d'Implémenter des contrôles pour répondre à l'Objectif de l'Approche Personnalisée de l'exigence d'une manière qui ne suit pas strictement l'exigence définie. Comme chaque implémentation personnalisée diffère, il n'existe pas de procédures de test définies ; à la place, l'évaluateur doit dériver des procédures de test adaptées à l'Implémentation spécifique afin que l'évaluateur puisse valider que les contrôles implémentés répondent à l'objectif énoncé.

L'approche personnalisée est-elle une option pour toutes les exigences PCI DSS ?

La plupart des exigences PCI DSS peuvent être satisfaites en utilisant soit l'approche définie, soit l'approche personnalisée. Cependant, plusieurs exigences n'ont pas d'Objectif de l'Approche Personnalisée, ce qui entraîne l'absence d'option d'approche personnalisée.

Pour quel type d'entités l'approche personnalisée est-elle destinée ?

L'approche personnalisée est destinée à soutenir l'innovation dans les pratiques de sécurité, permettant aux entités une plus grande flexibilité pour démontrer comment leurs contrôles de sécurité répondent aux objectifs PCI DSS. Cette approche est recommandée pour les entités matures en matière de gestion des risques, qui démontrent une approche robuste de gestion des risques en sécurité, incluant, sans s'y limiter, un service dédié à la gestion des risques ou une approche de gestion des risques à l'échelle de l'entité.

Les contrôles implémentés et validés en utilisant l'approche personnalisée doivent répondre aux exigences ou dépasser le niveau de sécurité fourni par l'approche définie. Il en découle que le niveau de documentation et d'effort requis pour valider les implémentations personnalisées sera également plus élevé que pour l'approche définie.

Les entités qui remplissent un Questionnaire d'auto-évaluation (SAQ) peuvent-elles adopter une approche personnalisée ?

L'utilisation de l'approche personnalisée n'est pas prise en charge dans les Questionnaires D'auto-Évaluation (SAQ). Les entités souhaitant procéder à une validation selon l'approche personnalisée peuvent utiliser le modèle de Rapport de Conformité (ROC) PCI DSS pour consigner les résultats de l'évaluation. Les questions relatives à l'utilisation de l'approche personnalisée, notamment celles visant à savoir si les entités éligibles à un SAQ peuvent, à la place, remplir un ROC afin de recourir à une approche personnalisée, doivent toujours être adressées aux organismes chargés de la gestion des programmes de conformité, tels que les marques de paiement et les acquéreurs.

Quelle est la différence entre un contrôle compensatoire et l'approche personnalisée ?

Il est important de noter que les mesures de sécurité compensatoires ont un objectif différent de celui de l'approche personnalisée. Contrairement aux mesures de sécurité compensatoires, qui sont utilisés lorsque les organisations ont une contrainte et ne **peuvent pas** satisfaire l'exigence telle qu'énoncée, l'approche personnalisée est destinée aux entités qui choisissent de satisfaire l'exigence différemment de ce qui est indiqué. Dans ce cas, l'entité doit satisfaire l'Objectif de l'Approche Personnalisée énoncé au lieu de l'exigence énoncée. L'approche personnalisée est la plus réussie lorsque l'entité dispose de processus de sécurité robustes et de pratiques solides de gestion des risques, ainsi que de la capacité à concevoir efficacement la documentation, les tests et la maintenance des contrôles de sécurité qui répondent à cet objectif.

Veuillez noter que l'Objectif de l'Approche Personnalisée d'une exigence peut être examiné afin de comprendre l'intention de cette exigence, même lorsqu'une entité ne met pas en œuvre d'approche personnalisée pour cette exigence.

Peut-on utiliser à la fois des mesures compensatoires et une approche personnalisée pour répondre à la même exigence ?

Oui. Une entité peut utiliser des mesures de sécurité compensatoires pour certains composants du système et l'approche personnalisée pour satisfaire cette même exigence pour d'autres composants du système. En prenant l'Exigence 5.3.1 comme exemple, une entité pourrait utiliser un contrôle compensatoire pour satisfaire cette exigence pour un certain type de serveur, lorsqu'il existe une contrainte commerciale légitime et documentée empêchant ce serveur de satisfaire l'exigence énoncée. L'entité peut également choisir d'utiliser l'approche personnalisée pour satisfaire cette même exigence pour d'autres composants du système, lorsqu'elle a implémenté une approche unique pour détecter et traiter les dernières menaces de logiciels malveillants. L'entité pourrait également utiliser l'approche définie telle qu'énoncée pour satisfaire cette même exigence pour un autre groupe de composants du système.

Si une entité élabore une approche personnalisée qui ne répond pas à l'objectif de cette approche, peut-elle recourir à des mesures compensatoires pour atteindre cet objectif ?

Non. Les mesures compensatoires ne sont pas une option avec l'approche personnalisée. L'approche personnalisée est destinée aux organisations qui choisissent de développer leurs propres contrôles répondant à l'Objectif de l'Approche Personnalisée de l'exigence. Si une organisation développe une approche personnalisée et rencontre ensuite des contraintes techniques ou commerciales l'empêchant de satisfaire l'Objectif de l'Approche Personnalisée, cela signifie que l'organisation a conçu une approche personnalisée qu'elle n'est pas en mesure de satisfaire. C'est pourquoi les mesures de sécurité compensatoires ne constituent pas une option dans le cadre de l'approche personnalisée.

Si une entité détermine qu'elle ne peut pas satisfaire une exigence PCI DSS avec une approche personnalisée, et qu'elle a une contrainte technique ou commerciale l'empêchant de satisfaire l'exigence de l'Approche Définie telle qu'écrite, l'entité peut plutôt choisir d'implémenter un contrôle compensatoire basé sur l'exigence originale de l'Approche Définie.

Comparaison des Cas d'Usage : Exemples pour les Mesures de Sécurité Compensatoires et l'Approche Personnalisée

Ces exemples sont fournis uniquement pour différencier les cas d'usage où un contrôle compensatoire ou une approche personnalisée peut être envisagé. Ces cas d'usage ne sont pas destinés à illustrer des implémentations réelles ou des contrôles adaptés ou recommandés pour un environnement spécifique. L'entité doit toujours vérifier auprès de son auditeur et de l'entité à laquelle elle soumettra les documents attestant de sa conformité si les mesures compensatoires ou les contrôles personnalisés sont acceptables et peuvent être utilisés.

Traité par une Commande Compensatrice	Traité dans le cadre d'une Approche Personnalisée
Exigence 3.3.1.2 Les données SAD sont conservées après l'autorisation, car l'entité ne dispose pas de la technologie nécessaire pour empêcher leur conservation.	*Cette exigence ne peut pas faire l'objet d'une approche personnalisée.*
Exigence 3.5.1 En raison d'une contrainte technique, le numéro PAN ne peut être ni crypté ni rendu illisible d'une quelconque autre manière.	
Exigence 5.2.1 Les solutions anti-malware ne peuvent pas être déployées sur certains systèmes en raison de contraintes techniques.	**Exigence 5.2.1** Un mécanisme est en place pour détecter tous les logiciels malveillants et empêcher leur installation ou leur exécution.
Exigence 8.3.6 L'outil d'un fournisseur de services cloud ne permet pas de modifier les paramètres relatifs aux mots de passe, et les paramètres fournis ne sont pas conformes aux exigences PCI DSS. *Ce problème pourrait être résolu soit par un contrôle compensatoire, soit par une approche personnalisée, en fonction du type de commande implémenté.*	
	Exigence 11.3.1 Les vulnérabilités internes sont identifiées à l'aide d'une méthode autre que l'analyse interne des vulnérabilités.
Exigence 11.3.2 En raison d'une modification à venir de l'outil ASV, le prochain scan de vulnérabilités externes ne pourra pas être effectué dans les délais prévus.	*Cette exigence ne peut pas faire l'objet d'une approche personnalisée.*
	Exigence 11.5.1 Un mécanisme autre que les systèmes IDS/IPS est utilisé pour détecter le trafic réseau anormal.

Rôles des Mesures de Sécurité Compensatoires et de l'Approche Personnalisée

Rôle de l'Entité : Mesures de Sécurité Compensatoires

Les entités sont tenues de définir des mesures compensatoires lorsqu'elles y ont recours et de les documenter en remplissant une ou plusieurs Fiches de Travail relatives aux Mesures Compensatoires (CCW). Les CCW de l'entité doivent inclure :

- Contrainte(s) technique(s) et/ou commerciale(s) clairement définie(s) qui empêchent l'entité de se conformer à l'exigence PCI DSS telle qu'elle est énoncée.
- La définition du contrôle compensatoire et l'explication de la manière dont le contrôle répond aux objectifs de l'exigence d'origine et à tout risque accru : par exemple, en termes de personnes, processus, politiques et/ou technologies qui composent le contrôle.
- Objectif du contrôle d'origine :
  - L'entité peut, sans y être obligée, utiliser l'Objectif de l'Approche Personnalisée de l'exigence pour cet objectif.
- Objectif atteint grâce au contrôle compensatoire :
  - Il peut s'agir, sans que cela soit obligatoire, de l'objectif déclaré de l'Approche Personnalisée pour l'exigence PCI DSS.
- Une description de tout risque supplémentaire lié à l'absence du contrôle d'origine. La documentation doit refléter une compréhension de ce risque et de la manière dont il est traité.
- Une explication de la manière dont l'entité valide et teste le contrôle compensatoire.
- Une définition des processus et contrôles que l'entité a mis en place pour maintenir le contrôle compensatoire.

Un exemple de CCW est inclus dans PCI DSS v4.x dans l'*Annexe C* : *Fiche de Travail relatives aux Mesures de Sécurité Compensatoire**s*** Un modèle de *Fiche de Travail* relative au *Contrôle Compensatoire Supplémentaire* est disponible sur le site web du PCI SSC, dans la Bibliothèque de Documents sous la rubrique PCI DSS.

Rôle de l'Évaluateur : Mesures de Sécurité Compensatoires

Les évaluateurs sont tenus d'examiner minutieusement les Fiches de Travail relatives au Contrôle Compensatoire (CCW) de l'entité lors de chaque évaluation annuelle PCI DSS afin de s'assurer que ces fiches documentent et traitent de manière claire et efficace les éléments figurant dans *l'Annexe* C : *Fiche de Travail* relatives aux *Mesures de Sécurité Compensatoires, mentionnée ci-dessus dans la section « Rôle de l'Entité ».*

Pour la contrainte technique ou commerciale légitime documentée de l'entité, l'évaluateur n'est pas censé confirmer que la contrainte commerciale ou technique est valide, mais uniquement que la contrainte est entièrement documentée par l'entité. Cependant, l'évaluateur est censé tester les éléments de contrôle implémentés par l'entité pour confirmer que la mesure compensatoire est en place et fonctionne efficacement.

L'évaluateur est censé :

- Inclure les CCW de l'entité dans le Rapport de Conformité (ROC) ou dans le Questionnaire d'auto-évaluation (SAQ), selon le cas.
- Effectuer des tests du contrôle compensatoire, y compris examiner les paramètres de configuration, examiner la documentation, observer les processus, etc., selon ce qui s'applique à l'exigence et au contrôle concernés.
  - Les Procédures de Test de l'exigence peuvent être considérées comme un guide du type de test attendu pour cette exigence.
- Lors de la complétion d'un ROC, pour chaque exigence PCI DSS satisfaite par un contrôle compensatoire :
  - Cochez la case « Mesures compensatoires ».
  - Inclure une description de la manière dont les tests et les preuves de l'évaluateur démontrent que l'exigence est en place.
  - Documenter les tests effectués dans les dossiers de travail de l'évaluateur et conserver les preuves avec les autres preuves d'évaluation.

Une mesure compensatoire peut-elle être utilisée pour traiter une exigence qui a été manquée dans le passé ?

Non. Pour PCI DSS v4.x, Annexe B : Les Mesures Compensatoires ont été mises à jour afin de préciser qu'elles ne peuvent pas être utilisées pour remédier rétroactivement à une exigence qui n'avait pas été respectée par le passé. Il n'a jamais été prévu que les mesures de sécurité compensatoires puissent être utilisés de cette manière. Par exemple, une tâche qui aurait dû être effectuée ne l'a pas été, et aucune action n'a été entreprise à ce moment-là pour y remédier. Cependant, une entité peut implémenter un contrôle compensatoire pour traiter des facteurs susceptibles d'affecter l'exécution future d'une tâche (par exemple, anticiper une interruption planifiée du système ou les congés du personnel).

Une mesure compensatoire peut-elle être utilisée pour satisfaire plusieurs exigences PCI DSS ?

Oui. Un contrôle compensatoire peut être conçu pour atténuer le risque de ne pas satisfaire plus d'une exigence. Cependant, la manière dont chaque exigence est satisfaite par ce contrôle compensatoire doit être documentée séparément dans des Fiches de Travail relatives aux Mesures Compensatoires individuelles.

Tous les objectifs et risques associés à chaque exigence doivent être pris en compte, et les mesures compensatoires doivent être validées de manière indépendante pour chaque exigence.

Une mesure compensatoire doit-elle être utilisée uniquement pour une durée limitée ?

Non. Il n'existe aucune exigence stipulant qu'un contrôle compensatoire ne peut être en place que pour une durée limitée ; cependant, l'entité évaluée doit examiner ses Mesures de Sécurité Compensatoires chaque année pour confirmer que les contrôles sont toujours efficaces et nécessaires. Par exemple, une nouvelle technologie ou un nouveau système peut nécessiter un contrôle compensatoire révisé pour répondre à l'objectif de l'exigence, ou peut avoir supprimé le besoin d'un contrôle compensatoire, permettant ainsi de satisfaire l'exigence PCI DSS d'origine telle qu'énoncée.

De même, l'évaluateur est censé examiner les mesures de sécurité compensatoires de l'entité chaque année pour confirmer qu'ils sont toujours appropriés et nécessaires pour traiter le risque et satisfaire l'exigence.

Rôle de l'Entité : Approche Personnalisée

L'entité évaluée conçoit, développe, analyse, implémente et maintient ses contrôles personnalisés, y compris les étapes suivantes :

- Consultez les informations relatives à l'approche personnalisée figurant dans la section Références et Matériels d'Appui de ce document.
- Définissez et documentez chaque mesure de contrôle personnalisée, en précisant notamment en quoi cette mesure répond à l'objectif de l'exigence. Consultez le *Exemple de Modèle de Matrice de Mesures de Sécurité*[1] pour obtenir un modèle pouvant être utilisé afin de consigner les informations relatives au contrôle personnalisé.
- Réalisez et consignez une analyse de risque ciblée démontrant que le contrôle personnalisé est suffisamment solide pour offrir une protection au moins équivalente à celle prévue par l'Exigence Définie. Reportez-vous à l'Exemple de Modèle D'analyse Ciblée de Risques Modèle[1] pour obtenir un modèle pouvant être utilisé afin de consigner les informations relatives au contrôle personnalisé.
- Réalisez et documentez des tests confirmant que chaque contrôle personnalisé répond efficacement à l'objectif de l'exigence. Reportez-vous à *l'Exemple de Modèle de Matrice de Mesures de Sécurité* Types pour documenter les tests effectués et leurs résultats.
- Décrivez comment l'efficacité de chaque contrôle est surveillée et maintenue au fil du temps.
- Communiquez dès que possible avec votre évaluateur au sujet de vos projets pour implémenter une approche personnalisée.
- Fournissez à votre évaluateur toute la documentation relative à chaque contrôle personnalisé.

Pour que l'entité évaluée puisse implémenter et maintenir efficacement ses contrôles sur mesure, il est important qu'elle s'approprie pleinement la responsabilité de ces contrôles et qu'elle s'y engage activement.

Rôle de l'Évaluateur : Approche Personnalisée

Lorsque l'approche personnalisée est utilisée, les évaluateurs doivent s'attendre à recevoir au préalable la documentation relative à cette approche personnalisée fournie par l'entité, afin de les aider à mener à bien les étapes suivantes :

- Vérifier que l'exigence PCI DSS concernée est éligible à l'approche personnalisée.
- Examiner la documentation de l'entité afin de bien comprendre le contrôle personnalisé.
  - Vérifier qu'une Matrice des Contrôles et une Analyse des Risques Ciblée ont bien été établies et fournies.

[1] Deux modèles sont inclus dans Modèles Types : Approche Personnalisée – 1) une Approche Personnalisée – Modèle de Matrice de Contrôles et 2) une Approche Personnalisée – Exemple de Modèle D'analyse Ciblée de Risques. Ce document est disponible sur le site web du PCI SSC, dans la bibliothèque de documents, sous PCI DSS. Bien qu'il ne soit pas obligatoire pour les entités de respecter les formats spécifiques de ces modèles, la Matrice de Contrôle de l'Approche Personnalisée et l'Analyse des Risques Ciblés de l'entité doivent inclure toutes les informations figurant dans ces modèles, conformément à l'exigence 12.3.2 du PCI DSS.

- Vérifier que chaque contrôle personnalisé est suffisamment documenté, notamment que :
  - La documentation comprend toutes les informations requises, telles que spécifiées dans les modèles de Matrice des Contrôles et d'Analyse des Risques Ciblée de l'Approche Personnalisée.
  - La documentation décrit comment le contrôle personnalisé offre une protection au moins équivalente à celle de l'Exigence Définie.
- Examiner les tests effectués par l'entité sur le contrôle sur mesure ainsi que leurs résultats afin de déterminer si ces tests étaient suffisants pour évaluer de manière approfondie les contrôles.
- Élaborer des procédures de test rigoureuses permettant de tester de manière approfondie chaque contrôle sur mesure.
  - La documentation fournie par l'entité doit être suffisamment détaillée pour permettre à l'évaluateur de comprendre le fonctionnement du contrôle et d'élaborer des procédures de test appropriées.
  - Si l'évaluateur estime que les tests de l'entité ont permis une évaluation approfondie du contrôle, il peut, s'il le souhaite, s'appuyer sur les tests de l'entité pour effectuer ses propres tests visant à vérifier l'efficacité du contrôle. Dans ce cas, l'évaluateur doit utiliser un échantillon différent de celui utilisé par l'entité.
- Effectuer des tests indépendants de chaque implémentation de contrôle personnalisé. Ne pas s'appuyer uniquement sur les résultats des tests de l'entité. L'objectif des tests de l'évaluateur est de déterminer si le contrôle :
  - Répond à l'Objectif de l'Approche Personnalisée de l'exigence,
  - Est maintenu pour garantir une efficacité continue, et
  - Est suffisant pour aboutir à une conclusion « sur place ».
- Documenter chaque contrôle personnalisé dans le Rapport de Conformité (ROC), à la fois-au niveau de l'exigence et dans l'Annexe E du ROC : *Modèle d'Approche Personnalisée.*
  - Lors d'une évaluation, l'évaluateur complète cette annexe pour chaque instance où un contrôle personnalisé est utilisé pour satisfaire une exigence PCI DSS.
  - En plus d'inclure les informations relatives au contrôle personnalisé provenant de la documentation de l'entité, l'évaluateur est censé inclure des détails sur les procédures de test dérivées par l'évaluateur, les preuves examinées par l'évaluateur pour confirmer que le contrôle est en place et fonctionne efficacement, et les résultats des tests effectués par l'évaluateur.

Dans le cadre de l'approche personnalisée, les tests effectués par l'entité peuvent-ils se substituer à ceux réalisés par l'évaluateur ?

Non. Les tests effectués par l'entité sont requis dans le cadre de l'implémentation et de la maintenance de l'approche personnalisée afin de démontrer l'efficacité du contrôle, mais ne remplacent pas les tests dérivés par l'évaluateur. L'évaluateur doit effectuer des tests indépendants et baser ses conclusions de validation sur les résultats de ces tests. Si l'évaluateur détermine que les tests de l'entité ont fourni une évaluation approfondie du contrôle, l'évaluateur peut utiliser le même test mais avec un ensemble d'échantillons différent de celui utilisé par l'entité.

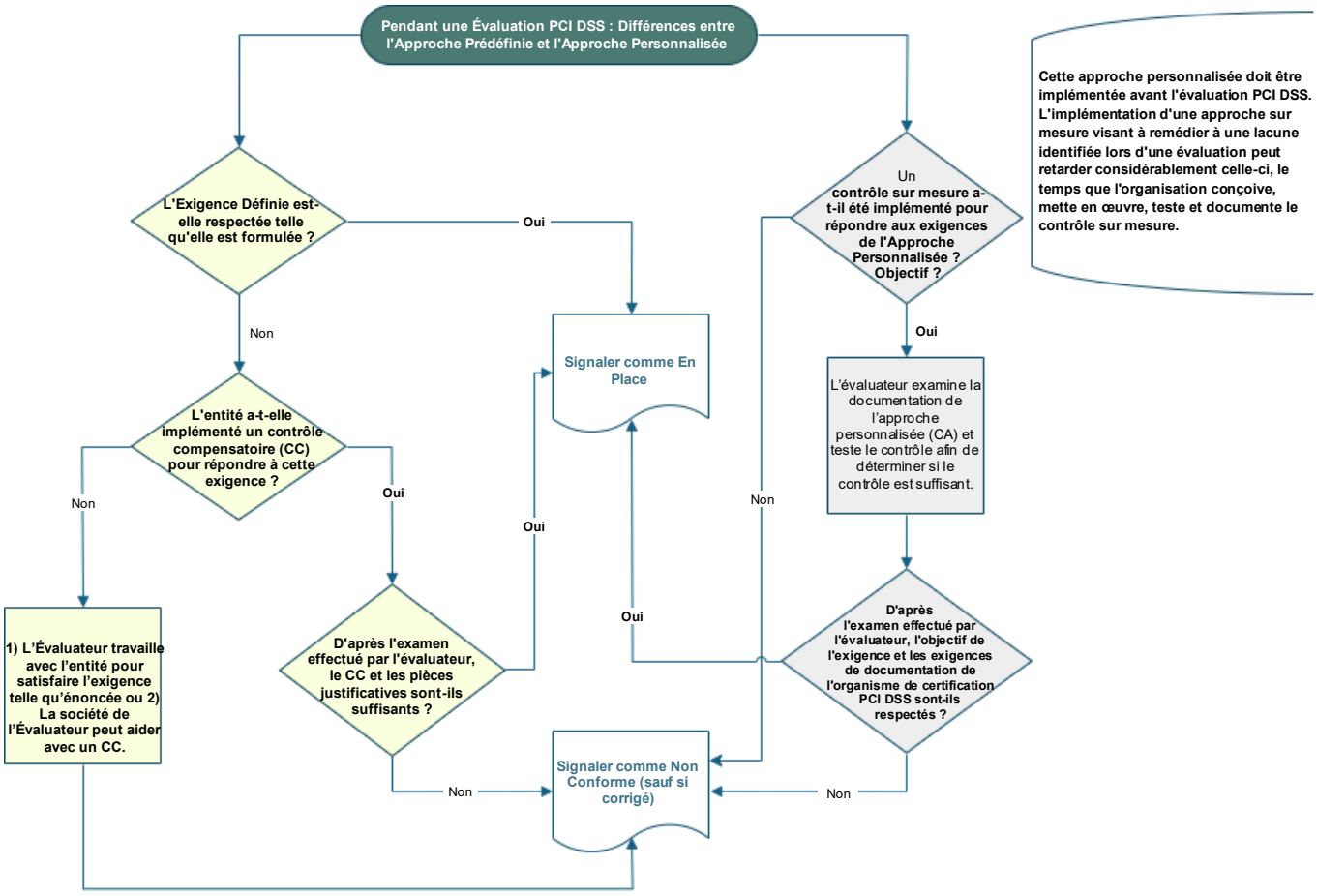
Pourquoi une approche personnalisée nécessite-t-elle davantage de documentation qu'une mesure compensatoire ?

Les implémentations personnalisées varient selon la conception et l'environnement et sont entièrement conçues par l'entité évaluée. Comme le contrôle est conçu par l'entité et donc non défini dans PCI DSS, il n'existe également aucune procédure de test prédéfinie. C'est pourquoi il est essentiel que la documentation de l'entité soit complète : elle doit définir ce qu'est le contrôle, comment il est implémenté, quel est le risque, comment ce risque est traité, comment le contrôle est testé par l'entité, comment le contrôle répond à l'objectif énoncé, comment l'entité s'assure que le contrôle reste efficace de manière continue, etc.

Cette documentation permet à l'évaluateur de comprendre pleinement le contrôle et son fonctionnement afin qu'il puisse dériver des procédures de test appropriées et valider indépendamment le contrôle.

Le diagramme ci-dessous illustre comment l'approche des mesures compensatoires et de l'approche personnalisée diffère lors d'une évaluation PCI DSS.

Figure 1 : En quoi l'Approche Définie et l'Approche Personnalisée diffèrent-elles lors d'une Évaluation PCI DSS ?



Documenter les Mesures Compensatoires et l'Approche Personnalisée

Les entités sont encouragées à préparer une documentation claire, complète et bien structurée pour leurs mesures compensatoires ou personnalisés. Une documentation complète fournit aux évaluateurs une base solide pour comprendre et évaluer le contrôle, l'environnement et la manière dont le contrôle répond à l'intention de l'exigence ou de l'objectif PCI DSS.

La qualité de la documentation de l'entité affecte directement la capacité de l'évaluateur à valider les contrôles et à parvenir à une conclusion défendable.

Pour les mesures compensatoires comme pour les implémentations personnalisées, la documentation de l'entité doit :

- Être complète, claire et compréhensible pour un lecteur indépendant.
- Se suffire à elle-même sans dépendre d'un contexte non documenté.
- Démontrer clairement comment les objectifs sont atteints et comment les risques sont traités.
- Inclure des preuves de la manière dont l'entité a confirmé que le contrôle fonctionne efficacement, y compris des détails sur les processus de l'entité et les résultats liés à la validation, aux tests et à l'assurance continue.

Une mesure compensatoire ou une approche personnalisée peut-elle être validée si la documentation ou les preuves de l'entité sont incomplètes ?

Non. Si la documentation n'est pas suffisante, l'évaluateur peut être incapable de valider que le contrôle est conçu et fonctionne efficacement. Si l'entité ne fournit pas suffisamment de preuves à l'évaluateur, ou si l'évaluateur n'a pas l'assurance que la documentation et les contrôles de l'entité sont suffisants, l'évaluateur peut déterminer qu'un résultat « Non mis en place » est approprié.

Indépendance de l'évaluateur

L'indépendance de l'évaluateur est un principe fondamental des évaluations PCI DSS et s'applique également lors de la validation des mesures compensatoires et des implémentations personnalisées. L'entité évaluée est responsable du développement, de l'implémentation et de la maintenance des mesures compensatoires.

Les QSA peuvent-ils concevoir ou implémenter des contrôles au nom d'une organisation ?

Bien que les employés QSA puissent aider les entités dans la conception ou l'implémentation de contrôles, les entreprises QSA doivent respecter les exigences d'indépendance définies dans les *Exigences de Qualification QSA* et le *Guide du Programme QSA*. Cela inclut la mise en place de contrôles de séparation des tâches pour garantir que les employés QSA réalisant ou aidant à une évaluation PCI DSS sont indépendants et ne sont soumis à aucun conflit d'intérêts.

Il serait un conflit d'intérêts pour un Employé QSA ayant participé à la conception ou à l'implémentation d'un contrôle de tester, évaluer ou aider à l'évaluation d'un contrôle compensatoire ou personnalisé. Se référer à la *FAQ 1562*, « Is a QSA Employee that designs, develops, or implements specific controls for a customer also permitted to assess those same controls? » sur la page des FAQs du PCI SSC pour plus d'informations.

En particulier pour l'Approche Personnalisée

Bien qu'un employé QSA puisse fournir des services de conseil liés à l'approche personnalisée, une organisation qui a besoin d'un QSA pour concevoir ou implémenter ses contrôles personnalisés peut ne pas être un bon candidat pour l'approche personnalisée, car il peut être difficile pour l'organisation de maintenir ce contrôle et de garantir qu'il continue de fonctionner efficacement. Une organisation ayant une maturité en gestion des risques, un engagement et les ressources nécessaires pour développer, implémenter et maintenir ses propres contrôles personnalisés est plus susceptible d'atteindre une efficacité de sécurité à long terme avec des contrôles personnalisés.

Toute implication d'un évaluateur ou d'une Entreprise QSA dans le développement de mesures compensatoires ou personnalisés doit être documentée dans la Section 1.4 du Rapport de Conformité (ROC).

Références et Matériels d'Appui

Se référer aux sections et annexes PCI DSS v4.x suivantes, ainsi qu'aux documents d'orientation, modèles et formulaires suivants :

Pour l'Approche Personnalisée

- La Section Introductive 8 de PCI DSS v4.x compare les mesures compensatoires et l'approche personnalisée et fournit des aperçus des deux approches.
- L'Annexe D de PCI DSS v4.x fournit plus de détails sur l'approche personnalisée, y compris les éléments de l'analyse de risque ciblée requise et les responsabilités de l'entité et de l'évaluateur.
- Dans le PCI DSS v4.x, la *Figure 5 Comprendre les Parties des Exigences* indique l'emplacement, au sein de chaque exigence, de l'Exigence d'Approche Définie et, le cas échéant, de l'Objectif d'Approche Personnalisée.
- L'exigence 12.3.2, relative à une Analyse Ciblée des Risques (TRA) pour toute exigence PCI DSS satisfaite par une approche personnalisée, définit les éléments d'une TRA dans le cadre d'une approche personnalisée.
- Le Modèle de Rapport de Conformité PCI DSS 4.x, Annexe E : Modèle d'Approche Personnalisée.
- *Modèles Types* : Approche *Personnalisée* est disponible sur le site web du PCI SSC, dans la Bibliothèque de documents sous PCI DSS. Ce document comprend :
  - Approche Personnalisée - Modèle Type de Matrice des Contrôles
  - Approche Personnalisée - Modèle Type d'Analyse Ciblée des Risques
- *PCI DSS v4.x : Guide d'Analyse des Risques Ciblés* – Décrit les deux types d'analyses des risques ciblés (TRA) inclus dans le PCI DSS v4.x.

Pour les Mesures Compensatoires

- Dans le PCI DSS v4.x :
  - Section d'Introduction 8, qui compare les mesures compensatoires et l'approche personnalisée et fournit une vue d'ensemble des deux approches.
  - *Annexe B : Mesures Compensatoires*, qui fournit la définition et les critères de base.
  - *Annexe C : Fiche D'Identification des Mesures Compensatoires,* un exemple de fiche de travail que les entités utilisent pour définir les mesures compensatoires lorsqu'elles s'en servent pour satisfaire à une exigence de PCI DSS.
- Une *Fiche de Travail Supplémentaire relatives aux Mesures Compensatoires,* destinée aux entités pour documenter leurs mesures compensatoires, est disponible sur le site web du PCI SSC, dans la Bibliothèque de Documents sous PCI DSS.

Annexe : Exemples de Modèles Complétés de Mesures Compensatoires et d'Approche Personnalisée

Exemple Complet pour l'Entité : Fiche D'Identification des Mesures Compensatoires

Veuillez noter que ce document n'est fourni qu'à titre d'exemple illustrant l'une des façons de remplir une Fiche de Travail relative aux Mesures de Sécurité Compensatoires et ne constitue en aucun cas un exemple de contrôle concret adapté à un environnement spécifique ou dont l'utilisation serait recommandée dans un tel contexte.

Numéro et Définition de l'Exigence : Exigence 8.4.2 du PCI DSS – L'authentification multifactorielle (MFA) est implémentée pour tous les accès à l'Environnement de Données Relatives au Titulaire de Carte (CDE).

	Informations Requises	Explication
1. Contraintes	Décrire les contraintes techniques ou commerciales légitimes qui empêchent de respecter l'exigence initiale.	ABC Org exploite une plateforme d'autorisation de paiement héritée (ID du Système : PCIPAY-AUTH-01) fonctionnant sous une version propriétaire d'UNIX 5.2. Cette plateforme ne prend pas en charge l'intégration avec les mécanismes modernes d'authentification à plusieurs facteurs (MFA), notamment les modules MFA basés sur RADIUS, SAML ou PAM. La plateforme bénéficie d'une assistance technique de la part du fournisseur, mais ne peut être modifiée sans compromettre cette assistance et l'intégrité du système. Le remplacement de ce système est prévu dans le cadre du projet PCIPAY-MODERN-02, dont l'achèvement est prévu pour le T4 2027.
2. Définition des Mesures Compensatoires	Définir les mesures compensatoires : expliquer comment elles répondent aux objectifs de la mesure d'origine et au risque accru, le cas échéant.	L'organisation ABC a implémenté les mesures compensatoires suivantes : **Application de la Politique MFA des Serveurs de Rebond** Tout accès à PAY-AUTH-01 est limité aux « jump hosts » administratifs dédiés situés dans le segment de réseau VLAN-SEC-ADM. Pour accéder aux « jump hosts », il faut : ▪ ID utilisateur unique ▪ Authentification par mot de passe ▪ Jeton d'authentification matériel (périphérique certifié FIPS) ▪ Intégration de l'authentification Active Directory **Contrôles d'Accès au Réseau** Les règles du pare-feu limitent l'accès à PAY-AUTH-01 exclusivement depuis des « jump hosts ». L'accès direct depuis les postes de travail des utilisateurs, les connexions VPN ou d'autres segments du réseau est techniquement empêché.

	Informations Requises	Explication
		Référence du jeu de règles du pare-feu : FW-RULE-SET-CDE-ADM-V3. Surveillance et Journalisation des Sessions Toutes les sessions d'administration sont : ▪ Journalisées de manière centralisée ▪ Transmises à la plateforme SIEM de l'entreprise (SecurityLog-SIEM-01) ▪ Conservées pendant au moins 12 mois Enregistrement des Sessions Les sessions d'administration vers PAY-AUTH-01 sont enregistrées à l'aide de la solution de gestion des accès privilégiés (PAM) PAM-SEC-01. Les enregistrements de sessions sont conservés à des fins d'analyse forensique et de surveillance. Surveillance de la Sécurité et Alertes Le SIEM génère des alertes en cas de : ▪ Tentatives d'accès non autorisées ▪ Accès en dehors des plages horaires d'administration définies ▪ Tentatives d'escalade des privilèges Les alertes sont examinées par le personnel du SOC.
3. Objectif	Définir l'objectif du contrôle d'origine.	Assurer une authentification forte pour l'accès au CDE grâce à l'utilisation de plusieurs facteurs d'authentification.
	identifier l'objectif atteint par les mesures compensatoires. ***Remarque :*** *Il peut s'agir, sans que cela soit obligatoire, de l'objectif de l'Approche Personnalisée indiqué pour cette exigence dans le PCI DSS.*	Les mesures compensatoires répondent à l'objectif fixé en imposant l'authentification multifactorielle (MFA) avant d'accorder l'accès à PCIPAY-AUTH-01 et en empêchant tout accès direct au système.
4. Risque Identifié	Identifier tout risque supplémentaire posé par l'absence de la mesure de sécurité d'origine.	Les risques liés à l'impossibilité d'implémenter l'authentification multifactorielle (MFA) directement sur PCIPAY-AUTH-01 sont les suivants : ▪ Risque de compromission des identifiants d'authentification ▪ Accès non autorisé aux systèmes contenant les données des titulaires de carte Les mesures compensatoires implémentées atténuent ce risque en garantissant que : ▪ L'authentification MFA est obligatoire avant tout accès ▪ L'accès direct est empêché ▪ Tous les accès sont surveillés, consignés et examinés Le risque résiduel est évalué comme Faible.

	Informations Requises	Explication
5. Validation des Mesures Compensatoires	Définir la manière dont les mesures compensatoires ont été validées et testées.	L'entité valide l'efficacité des mesures compensatoires par les moyens suivants : ▪ Examens trimestriels des règles de pare-feu (Preuve : FW-Review-Reports) ▪ Des revues trimestrielles des accès privilégiés (Preuve : Access-Review-Records) ▪ Une vérification trimestrielle de l'application de l'authentification multifactorielle (MFA) sur les « jump hosts » ▪ Une vérification mensuelle des alertes SIEM ▪ Un audit interne annuel des contrôles d'accès privilégiés L'entité a examiné ces éléments de validation afin de s'assurer de l'efficacité du contrôle : ▪ Configurations du pare-feu ▪ Configurations du contrôle d'accès ▪ Rapports d'alertes SIEM ▪ Journaux d'enregistrement des sessions
6. Maintenance	Définir le ou les processus et les mesures en place pour maintenir les mesures compensatoires.	L'entité garantit l'efficacité des mesures compensatoires grâce à : ▪ Des procédures de gestion des changements régissant les modifications de configuration des pares-feux et des serveurs de rebond ▪ Une surveillance SIEM continue ▪ Des examens trimestriels des droits d'accès ▪ Un examen annuel de l'applicabilité des mesures compensatoires Responsable de l'examen des mesures compensatoires : Responsable de la Sécurité de l'Information Fréquence de l'examen : Annuelle

Exemple Complet pour l'Entité : Matrice des Contrôles pour une Approche Personnalisée

Veuillez noter que ce document n'est fourni qu'à titre d'exemple illustrant l'une des façons de remplir une Fiche de Travail relative aux Contrôles Compensatoires et ne constitue en aucun cas un exemple de contrôle concret adapté à un environnement spécifique ou dont l'utilisation serait recommandée dans un tel contexte.

Modèle de Matrice de Contrôle pour une Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée		
Nom/identifiant personnalisé du contrôle	Identification et Authentification Vocales	
Numéro(s) et objectif(s) des Exigences PCI DSS auxquels répondent ce(s) contrôle(s)	Exigence n° : 8.2.8	**Objectif :** Une session utilisateur ne peut être utilisée que par l'utilisateur autorisé.
Détails du ou des contrôle(s)		
Quel(s) contrôle(s) avons-nous implémenté(s) ?	L'entité exploite un environnement « Zero Touch » à des fins d'hygiène opérationnelle. Plutôt que de se connecter à l'aide d'un clavier, les utilisateurs de cet environnement se contentent de donner des commandes vocales à leur ordinateur. Lors de sa première connexion au système, l'utilisateur prononce la commande vocale « Reconnaître le nom d'utilisateur », par exemple « Reconnaître Alice ». Le système identifie et authentifie d'abord l'utilisateur grâce à son empreinte vocale unique, puis par le biais d'une requête adressée au système de contrôle d'accès physique, qui vérifie que l'utilisateur se trouve bien physiquement dans le lieu concerné. Il demandera ensuite à l'utilisateur (par exemple, Alice) de répéter trois mots choisis au hasard affichés à l'écran afin d'empêcher toute utilisation d'un enregistrement préalable et d'effectuer une deuxième vérification de l'empreinte vocale. À ce stade, l'utilisateur est connecté. Le système reste à l'écoute en permanence des commandes vocales. La session de l'utilisateur connecté reste active tant que celui-ci se trouve dans la zone physique ; elle prend fin dès qu'il utilise sa carte d'accès pour quitter la zone. Chaque fois que l'utilisateur émet une commande, son empreinte vocale est vérifiée. Si celle-ci ne correspond pas à celle de l'utilisateur connecté, la commande est rejetée et enregistrée. Les journaux sont traités par le SIEM. Si un autre utilisateur tente d'utiliser le terminal sur lequel l'utilisateur est connecté, l'empreinte vocale ne correspondra pas et le système rejettera la commande.	

Modèle de Matrice de Contrôle pour une Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée	
	Par exemple, si Dave (qui est un utilisateur autorisé du système, mais qui n'est pas connecté au terminal d'Alice) ou Mary (une personne malveillante) s'approche du système d'Alice et dit « Ouvre les portes du compartiment des capsules », l'ordinateur reconnaîtra que la commande n'a pas été émise par Alice et répondra « Je crains de ne pas pouvoir le faire », tout en enregistrant une tentative d'accès non autorisée. De plus, les interfaces USB et Bluetooth sont désactivées sur les systèmes, de sorte que le système de reconnaissance vocale ne peut pas être contourné manuellement.
Où le ou les contrôles sont-ils implémenté(s) ?	Site de production 17. Nevada.
Quand le(s) contrôle(s) est-il (sont-ils) effectué(s) ?	À chaque fois qu'une requête vocale est analysée.
Qui assume la responsabilité générale et rend compte du(des) contrôle(s) ?	Le Responsable de la sécurité de l'information
Qui participe à la gestion, à la maintenance et à la surveillance du(des) contrôle(s) ?	Le service chargé de l'inscription aux opérations sécurisées est responsable de l'intégration des nouveaux utilisateurs du système, ce qui inclut la formation des utilisateurs et la collecte d'échantillons vocaux suffisants pour établir une empreinte vocale fiable. La gestion et la maintenance du système sont externalisées à Acme Voiceprint Security Technologies, qui est gérée conformément à l'exigence 12.8 et fournit également cette technologie à de nombreuses institutions financières de premier plan à des fins de détection et de validation des fraudes, ainsi que d'accès aux informations clients dans les centres de contact.
Pour chaque exigence PCI DSS à laquelle le ou les contrôle(s) répond(ent), l'entité fournit des détails sur les éléments suivants :	
L'entité décrit en quoi le ou les contrôle(s) implémenté(s) répond(ent) à **l'objectif** de l'exigence PCI DSS.	Seul l'utilisateur connecté peut utiliser une session, car celui-ci est en effet réauthentifié (par reconnaissance vocale biométrique) à chaque fois qu'une commande est émise. Les autres utilisateurs autorisés et les utilisateurs non autorisés ne peuvent pas utiliser la session en cours.
L'entité décrit les tests qu'elle a **effectués** ainsi que leurs résultats, qui démontrent que le ou les contrôles répondent à l'objectif de l'exigence applicable.	Une évaluation de sécurité a été confiée à Acme Secure Testing Services afin de valider le fonctionnement du système et de tenter d'obtenir un accès non autorisé à une session utilisateur. Cette société n'y est pas parvenue. Par ailleurs, cette même société a mené un exercice de type « red team » et n'a pas non plus réussi à compromettre le système ni à obtenir un accès non autorisé en se faisant passer pour un utilisateur autorisé utilisant la fonction vocale.

Modèle de Matrice de Contrôle pour une Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée	
L'entité décrit brièvement les résultats de l'analyse de risque distincte qu'elle a **réalisée**, qui explique le ou les contrôle(s) implémentés et décrit comment ces résultats vérifient que le ou les contrôle(s) offrent au moins un niveau de protection équivalent à celui de l'approche définie pour l'exigence PCI DSS applicable. Reportez-vous au modèle d'analyse de risque ciblée séparé pour plus de détails sur la manière de documenter cette analyse de risque.	Avec le contrôle défini par l'exigence, un utilisateur connecté pourrait s'absenter de son poste de travail et un acteur malveillant non autorisé disposerait de 15 minutes pour accéder au poste avant l'expiration de la session. Grâce à ce contrôle, la session reste toujours active lorsque l'utilisateur se trouve physiquement dans l'environnement, et l'empreinte vocale de chaque commande est validée comme provenant de l'utilisateur connecté avant que celle-ci ne soit exécutée. Le système traite donc un niveau de risque plus élevé que le contrôle de validation défini.
L'entité décrit les mesures qu'elle a implémentées pour garantir le maintien du ou des contrôle(s) et assurer leur efficacité de manière continue. *Par exemple, comment l'entité surveille l'efficacité des contrôles, comment les défaillances des contrôles sont détectées et traitées, ainsi que les mesures prises.*	Chaque mois, un membre de l'équipe GRC tente de prendre le contrôle d'une session utilisateur en émettant des commandes vocales dans les locaux et en utilisant des enregistrements vocaux préenregistrés. Cet exercice suit une procédure documentée, et les résultats sont enregistrés sous forme audio par le système. Les enregistrements audios et les journaux de procédure sont examinés par le Responsable de la Gouvernance, des Risques et de la Conformité après chaque test. Une procédure de signalement des incidents suspects est en place. Si un utilisateur soupçonne que le système a répondu à une voix n'appartenant pas à un utilisateur connecté, il doit suivre une procédure bien définie. Tous les utilisateurs ont été formés à l'utilisation de cette procédure et ont rempli un rapport d'incident fictif. Le recours à cette procédure fait partie de la formation annuelle à la sécurité des utilisateurs. À ce jour, aucun incident n'a été signalé.

Exemple Complet pour l'Entité : Analyse Ciblée des Risques pour l'Approche Personnalisée

Veuillez noter qu'il s'agit uniquement d'un exemple illustrant l'une des façons de réaliser une analyse ciblée des Risques dans le cadre d'une approche personnalisée, et non d'un exemple de mesure de contrôle concrète adaptée à un environnement spécifique ou dont l'utilisation serait recommandée dans un tel contexte.

Analyse Ciblée des Risques pour l'Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée	
Élément	**Détails**
1. Identifier l'exigence	
1.1 Identifier l'exigence PCI DSS telle qu'elle est formulée.	8.2.8 Si une session utilisateur reste inactive pendant plus de 15 minutes, l'utilisateur doit s'authentifier à nouveau pour réactiver le terminal ou la session.
1.2 Identifier l'objectif de l'exigence PCI DSS telle qu'elle est formulée.	Une session utilisateur ne peut être utilisée que par l'utilisateur autorisé.
1.3 Décrivez le risque que cette exigence vise à prévenir.	Un acteur malveillant, interne ou externe, peut prendre le contrôle de la session d'un utilisateur légitime laissée sans surveillance. Il serait alors en mesure d'effectuer des actions, d'accéder à des données et d'émettre des commandes, qui seraient attribuées à tort à l'utilisateur connecté. Un accès non autorisé aux systèmes et aux données pourrait se produire. Les fichiers journaux seraient inexacts, enregistrant l'identité de l'utilisateur connecté pour des actions qu'il n'a pas effectuées.
2. Décrivez la solution proposée	
2.1 Nom/identifiant du contrôle personnalisé	Identification et Authentification Vocales
2.2 Quels éléments de l'exigence, telle qu'elle est formulée, seront modifiés dans la solution proposée ?	Le système utilisé ne fait pas de distinction spécifique entre les états « actif » et « inactif » et n'est donc pas en mesure de détecter qu'une session est « inactive » depuis 15 minutes. En revanche, un utilisateur connecté peut émettre une commande vocale à tout moment après s'être initialement authentifié et connecté ; toutefois, chaque commande émise est vérifiée afin de s'assurer qu'elle provient bien de l'utilisateur connecté. Seules les commandes émises par l'utilisateur connecté sont acceptées.
2.3 Comment la solution proposée permettra-t-elle d'empêcher ces actes malveillants ?	Chaque commande vocale étant vérifiée avant d'être exécutée, toute commande émise par une personne autre que l'utilisateur connecté échouera à la vérification et ne sera pas prise en compte par le système. Cela empêche donc tout acteur malveillant, qu'il soit interne ou externe, de prendre le contrôle de la session laissée sans surveillance d'un utilisateur légitime.

Analyse Ciblée des Risques pour l'Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée						
Élément	**Détails**					
3. Analyser toute évolution de la PROBABILITÉ que l'acte malveillant se produise, entraînant une violation de la confidentialité des données des titulaires de carte						
3.1 Décrire les facteurs détaillés dans la Matrice de Contrôle qui influent sur la probabilité que l'acte malveillant se produise.	Chaque commande reçue par le système est validée comme ayant été émise par l'utilisateur connecté. Cela réduit la probabilité qu'une session connectée soit détournée par un acteur malveillant. Selon l'exigence définie, un acteur malveillant dispose d'un délai de 15 minutes pour accéder physiquement à une session authentifiée laissée sans surveillance et en prendre le contrôle. Parmi les contrôles déployés, il n'existe aucune possibilité pour un acteur malveillant d'émettre des commandes sous la session d'un utilisateur connecté.					
3.2 Décrivez les raisons pour lesquelles l'atteinte pourrait tout de même se produire après la mise en œuvre du contrôle personnalisé.	Le système a fait l'objet de tests approfondis et ne peut être contourné par des solutions technologiques telles que la synthèse vocale et la lecture d'enregistrements ; on prévoit d'ailleurs que même les tentatives en ce sens seraient remarquées par l'utilisateur connecté, qui doit être physiquement présent dans l'environnement pour rester connecté. Un acteur malveillant pourrait contourner le contrôle en intimidant physiquement l'utilisateur connecté ; toutefois, le système est équipé d'un dispositif de surveillance des situations d'urgence qui ne fournit aucune indication d'activation à l'utilisateur mais alerte le personnel de sécurité. Lors des exercices de test et d'évaluation de la sécurité, le système n'a pas pu être contourné par un attaquant simulé.					
3.3 Dans quelle mesure les contrôles détaillés dans l'approche personnalisée modifient-ils la probabilité que l'atteinte se produise par rapport à l'exigence de l'approche définie ?	Les actes de malice sont plus susceptibles de se produire	☐	Aucun changement	☐	Les actes de malice sont moins susceptibles de se produire	☒
3.4 Justifiez votre évaluation de l'évolution de la probabilité que l'incident se produise une fois les contrôles personnalisés mis en place.	Le délai de 15 minutes prévu par l'exigence pour qu'un acteur malveillant puisse prendre le contrôle de la session d'un utilisateur connecté est ramené à zéro minute, car chaque commande est validée comme provenant de l'utilisateur connecté.					
4. Analysez toute modification de l'IMPACT d'un accès non autorisé aux données de compte						
4.1 Pour l'ensemble des composants systèmes couverts par cette solution, quel volume de données de compte serait exposé à un risque d'accès non autorisé en cas de défaillance de la solution ?	**4.1.1** Nombre de PAN stockés	Aucun. L'entité ne stocke pas de PAN.	**4.1.2** Nombre de PAN traités ou transmis sur une période de 12 mois	32 millions		

Analyse Ciblée des Risques pour l'Approche Personnalisée – Exemple Complet À remplir par l'entité évaluée	
Élément	**Détails**
4.2 Description de la manière dont les contrôles personnalisés permettront directement : De réduire le nombre de numéros de carte (PAN) compromis en cas de réussite d'un acteur malveillant, et/ou De permettre une notification plus rapide des numéros de carte compromis aux marques de cartes.	Les contrôles mis en place ne réduisent en rien l'impact d'un accès non autorisé aux données des comptes.
5. Approbation et examen des risques	
5.1 J'ai examiné l'analyse des risques ci-dessus et je reconnais que l'utilisation de l'approche personnalisée proposée, telle que détaillée, offre un niveau de protection au moins équivalent à celui de l'approche définie pour l'exigence PCI DSS applicable.	[Signature]
5.2 Cette analyse des risques doit être examinée et mise à jour au plus tard à la date suivante :	[Date]

Exemple Complété à l'Intention de l'Évaluateur : Rapport de Conformité — Annexe E : Modèle d'Approche Personnalisée

Veuillez noter que ce document est fourni uniquement à titre d'exemple illustrant une manière de remplir le Rapport de Conformité et ne constitue pas un exemple de contrôle réel adapté à, ou recommandé pour une utilisation dans, un environnement spécifique.

Numéro et Définition de l'Exigence : Exigence PCI DSS 8.2.8 : Si une session utilisateur reste inactive pendant plus de 15 minutes, l'utilisateur doit s'authentifier à nouveau pour réactiver le terminal ou la session.

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur	
Indiquez-le nom/identifiant du contrôle personnalisé pour chaque contrôle utilisé pour répondre à l'objectif de l'approche personnalisée. *(**Remarque** : utilisez le nom du Contrôle Personnalisé figurant dans la matrice des contrôles de l'entité évaluée.)*	Identification et Authentification Vocales
Décrivez chaque contrôle utilisé pour répondre à l'objectif de l'Approche Personnalisée. *(Remarque : Reportez-vous aux Exigences et Procédures de Test du Payment Card Industry Data Security Standard (PCI DSS) pour l'Objectif de l'Approche Personnalisée.)*	Objectif : Une session utilisateur ne peut être utilisée que par l'utilisateur autorisé. 1. Les utilisateurs se connectent au système uniquement à l'aide de commandes vocales. Le système identifie et authentifie d'abord l'utilisateur grâce à son empreinte vocale unique, puis par le biais d'une requête adressée au système de contrôle d'accès physique, qui vérifie que l'utilisateur se trouve bien physiquement dans le lieu concerné. Le système demande ensuite à l'utilisateur de répéter trois mots choisis au hasard qui s'affichent à l'écran afin d'empêcher toute utilisation d'un enregistrement préalable, puis effectue une deuxième vérification de l'empreinte vocale. 2. Le système reste à l'écoute en permanence des commandes vocales. La session de l'utilisateur connecté reste active tant que celui-ci se trouve dans la zone physique ; elle prend fin dès qu'il utilise sa carte d'accès pour quitter la zone. 3. Chaque fois que l'utilisateur émet une commande, son empreinte vocale est vérifiée. Si celle-ci ne correspond pas à celle de l'utilisateur connecté, la commande est rejetée et enregistrée. Les journaux sont traités par le SIEM. 4. Si un autre utilisateur tente d'utiliser le terminal sur lequel l'utilisateur est connecté, l'empreinte vocale ne correspondra pas et le système rejettera la commande. 5. Les interfaces USB et Bluetooth sont désactivées sur les systèmes, de sorte que le système de

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur	
	reconnaissance vocale ne peut pas être contourné manuellement.
Décrivez-le ou les contrôle(s) utilisé(s) pour répondre à l'objectif de l'Approche Personnalisée.	Objectif de l'Approche Personnalisée : Une session utilisateur ne peut être utilisée que par l'utilisateur autorisé. Seul l'utilisateur connecté peut utiliser une session, car celui-ci est en effet réauthentifié (par reconnaissance vocale biométrique) à chaque fois qu'une commande est émise. Les autres utilisateurs autorisés et les utilisateurs non autorisés ne peuvent pas utiliser la session en cours.
Indiquez la documentation relative à la Matrice des Contrôles qui a été examinée et qui étaye une approche personnalisée pour cette exigence.	Doc-10 – Matrice des Contrôles pour une Approche Personnalisée
Indiquez la documentation relative à l'Analyse des Risques Ciblés qui a été examinée et qui étaye l'approche personnalisée pour cette exigence.	Doc-11 – Analyse des Risques Ciblés pour une Approche Personnalisée
Indiquez-le(s) nom(s) du (des) évaluateur(s) qui atteste(nt) que : L'entité a complété la Matrice de Contrôles en y incluant toutes les informations spécifiées dans le modèle de Matrice de Contrôles du PCI DSS v4.x : Les Modèles d'Exemples disponibles sur le site du PCI SSC pour Soutenir l'Approche Personnalisée, ainsi que les résultats de la Matrice de Contrôles, confirment que l'Approche Personnalisée répond à cette exigence. L'Entité a réalisé l'Analyse de Risque Ciblée, en incluant toutes les informations spécifiées dans le Modèle d'Analyse de Risque Ciblée du PCI DSS v4.x. Les Modèles d'Exemples destinés à Soutenir l'Approche Personnalisée sur le site du PCI SSC et le fait que les résultats de l'Analyse de Risque confirment l'utilisation de l'Approche Personnalisée pour cette exigence	Josephine Évaluatrice

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur		
Décrire les Procédures de Test dérivées et exécutées par l'Assesseur pour **valider que les contrôles mis en œuvre satisfont l'Objectif de l'Approche Personnalisée ;** par exemple pour déterminer si le ou les contrôles personnalisés sont suffisamment robustes pour offrir au minimum un niveau de protection équivalent à celui fourni par l'Approche Définie ***Remarque 1 :*** *Des contrôles techniques (par exemple, la vérification des réglages de configuration, de l'efficacité opérationnelle, etc.) doivent être effectués dans la mesure du possible et lorsque cela s'avère approprié.* ***Remarque 2 :*** Ajouter des lignes supplémentaires pour chaque procédure de test dérivée par l'évaluateur, selon les besoins. *Veillez à ce que toutes les lignes situées à droite de la rubrique « Procédure de test définie par l'Évaluateur » soient copiées pour chaque procédure de test définie par l'évaluateur qui est ajoutée.*		
Veuillez indiquer ici la procédure de test définie par l'évaluateur : 1.a) Après avoir obtenu l'accès à l'environnement tenter de se connecter au système via le clavier fourni si disponible 1.b) Après avoir obtenu l'accès à l'environnement tenter de se connecter au système via la commande vocale requise	**Identifiez ce qui a fait l'objet des tests** (par exemple, les personnes interrogées, les composants du système examinés, les processus observés, etc.) ***Remarque :*** *tous les articles testés doivent être identifiés de manière unique.*	Réalisé des tests avec l'assistance de Int-1, Int-2 et Int-3 dans l'environnement installation de production 17 Nevada sur ConsoleA et ConsoleB, où le Contrôle de l'Approche Personnalisée est actif. Parlé à Int-10, pour vérifier que les anomalies durant les tests de 1 et 2 ont été capturées et examinées.
	Identifiez tous les éléments de preuve examinés dans le cadre de cette procédure de test.	Examiné Doc-22 – journal SIEM pour la période des tests 1 et 2.

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur		
1.c) Après que l'utilisateur autorisé se connecte au système répéter les trois mots aléatoires affichés à l'écran 1.d) Après que l'utilisateur se connecte au système demander à un autre utilisateur autorisé de répéter les trois mots aléatoires affichés à l'écran 2.a) Avec l'utilisateur autorisé dans la pièce émettre une commande vocale en utilisant la voix de l'assesseur 2.b) Après que l'utilisateur autorisé a utilisé sa carte d'accès pour quitter la zone, émettre une commande vocale au système, en utilisant un enregistrement vocal de l'utilisateur donnant une commande. 3.a) Examiner les journaux du SIEM pour les résultats des tests 1 et 2. 3.b) Parler au personnel responsable de l'examen des journaux du SIEM pour déterminer s'ils ont capturé des anomalies durant les tests 1 et 2. 4.a) Testé en 2.b. 5.a) Examiner le système pour les interfaces USB et les capacités Bluetooth.	**Décrire les résultats** des tests effectués par l'Évaluateur pour cette procédure de test et comment ces résultats vérifient que les contrôles mis en œuvre répondent à l'Objectif de l'Approche Personnalisée.	L'Évaluateur a suivi un utilisateur autorisé dans les environnements contenant ConsoleA et ConsoleB. Test 5.a) D'abord, l'Évaluateur a examiné les consoles pour vérifier que les interfaces USB et les capacités Bluetooth du système n'étaient pas disponibles. Test 1.a) Ensuite, l'Évaluateur a observé qu'aucun clavier n'était disponible pour se connecter à l'une ou l'autre console. Test 1.b) L'Évaluateur a ensuite tenté de se connecter au système via la commande vocale requise. Le système a émis un message d'erreur indiquant que l'Évaluateur n'était pas un utilisateur autorisé et ne pouvait pas se connecter. Test 1.c) Ensuite, l'évaluateur a observé Int-1 se connecter à chaque console, notant l'utilisation d'une commande vocale acceptée par chaque console. L'évaluateur a ensuite répété les trois mots affichés à l'écran de chaque console et a noté que le système n'a pas connecté l'utilisateur et a affiché une erreur indiquant que la réponse vocale de l'utilisateur n'était pas reconnue. Test 1.d) L'évaluateur a observé Int-2 répéter les trois mots aléatoires affichés à l'écran. Le système a refusé de permettre à Int-2 d'accéder au système et a émis un avis indiquant que l'empreinte vocale ne correspondait pas. Test 2.a) Une fois Int-1 correctement connecté au système, et le système semblant répondre aux commandes de Int-1 pour ouvrir le fichier xyz, l'évaluateur a émis une commande au système pour ouvrir le fichier xyz. Le système a refusé d'ouvrir le fichier et a émis un message d'avertissement indiquant que l'empreinte vocale ne correspondait pas à l'utilisateur autorisé. Test 2.b & Test 4.a) L'évaluateur a observé l'utilisateur connecté utiliser sa carte d'accès pour quitter l'environnement. Après que l'utilisateur connecté a quitté l'environnement, l'évaluateur a tenté d'émettre une commande au système en utilisant un enregistrement de l'utilisateur précédent donnant une commande au système. Le système a refusé d'exécuter la commande et a émis une réponse indiquant que l'utilisateur avait été déconnecté du système.

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur		
		Test 3.a.) L'évaluateur a obtenu les journaux SIEM générés durant la période des tests et a vérifié que le système avait correctement journalisé les tentatives d'accès et de commande échouées. Test 3.b) L'évaluateur a interrogé Int-10 pour vérifier qu'elle avait reçu une alerte pour la tentative d'accès au système. L'évaluateur a déterminé que le contrôle, tel que conçu, fonctionne comme prévu et que la conception semble efficace pour limiter une session utilisateur uniquement à l'utilisateur ayant obtenu un accès autorisé.
Documenter les procédures de test dérivées et effectuées par l'évaluateur pour **valider que les contrôles sont maintenus afin d'assurer une efficacité continue** ; par exemple, comment l'entité surveille l'efficacité des contrôles et comment les défaillances de contrôle sont détectées, traitées et les actions entreprises. **Remarque 1 :** *Des contrôles techniques (par exemple, la vérification des réglages de configuration, de l'efficacité opérationnelle, etc.) doivent être effectués dans la mesure du possible et lorsque cela s'avère approprié.* **Remarque 2 :** Ajouter des lignes supplémentaires pour chaque procédure de test dérivée par l'évaluateur, selon les besoins. *Veillez à ce que toutes les lignes situées à droite de la rubrique « Procédure de test définie par l'Évaluateur » soient copiées pour chaque procédure de test définie par l'évaluateur qui est ajoutée.*		
Veuillez indiquer ici la procédure de test définie par l'évaluateur : 1) Examiner la procédure documentée du GRC pour tester les contrôles chaque mois. 2) Examiner la date et l'heure des résultats des 12 derniers mois pour vérifier que les tests sont effectués chaque mois.	**Identifiez ce qui a fait l'objet des tests** (par exemple, les personnes interrogées, les composants du système examinés, les processus observés, etc.) ***Remarque :*** *tous les articles testés doivent être identifiés de manière unique.*	Procédures du GRC (Doc-3) et résultats des tests des 12 derniers mois (Doc-4), Ont été interrogés Int-1 et ont examiné les résultats des tests de mars 2025 et d'août 2025 (Doc-16, Doc-17) Examen de la procédure documentée de signalement des incidents suspects avec Int-1. Examen des ressources pédagogiques relatives à la formation annuelle à la sécurité avec Int-1, Int-2 et Int-3. Examen des rapports d'incident fictifs complétés par Int-10 à Int-14. Il a été vérifié qu'aucun incident ne s'est produit au cours des 12 derniers mois.

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur		
3) Sélectionner deux résultats de test enregistrés pour vérifier que les contrôles ont fonctionné comme prévu et que le Responsable du GRC a examiné les résultats. 4) Examiner la procédure documentée de signalement d'incident suspect et vérifier que la procédure décrit suffisamment ce que le personnel doit faire dans le cas où le système répond à une voix non connectée. 5) Examiner les supports de formation annuelle à la sécurité pour vérifier que tous les utilisateurs ont été formés à l'utilisation de la procédure. 6) Sélectionner aléatoirement cinq rapports d'incident fictifs et les examiner pour en vérifier l'exhaustivité. 7) Si un incident vérifié s'est produit, examiner le rapport d'incident. Examinez tous les rapports d'incident vérifiés.	**Identifiez tous les éléments** de preuve examinés dans le cadre de cette procédure de test.	Test 1 : Doc-3 Test 2 : Doc-4 Test 3 : Doc-16, Doc-17, Int-01 Test 4 : Doc-20 Test 5 : Doc-23 Test 6 : Doc-50, 51, 52, 53, 54

Modèle de rapport de conformité pour l'Approche Personnalisée – Exemple Complété À remplir par l'évaluateur		
	Décrire les résultats des tests effectués par l'évaluateur pour cette procédure de test et comment ces résultats vérifient que les contrôles implémentés sont maintenus afin d'assurer une efficacité continue.	Les procédures du GRC pour tester les contrôles chaque mois semblent être claires et efficaces pour déterminer que les contrôles de commande vocale fonctionnent comme prévu. Le GRC a effectué les tests chaque mois, qui ont été enregistrés comme décrit dans les procédures. Les résultats semblaient être correctement documentés, y compris l'heure d'exécution, la personne ayant effectué le test et les résultats des tests. Les procédures de signalement d'incident suspect semblent être claires et adéquates. Les exigences de signalement incluent un formulaire (rapport d'incident) qui doit être utilisé par le personnel informatique dans l'Installation de production 17. Nevada. Il a été confirmé que l'ensemble du personnel informatique du site de production 17. Nevada a été formé en examinant le registre de formation obtenu auprès des RH. De plus, cinq rapports d'incident fictifs ont été sélectionnés aléatoirement dans les dossiers RH et il a été constaté qu'ils avaient été complétés conformément aux procédures. Nous avons examiné avec Int-1 le journal des incidents fourni par Int-1 pour les 12 derniers mois. Bien que des incidents aient été notés dans le journal, aucun ne semblait être lié au contrôle de commande vocale. Confirmation par Int-1 qu'aucun incident lié au contrôle n'a été signalé. Par conséquent, il semble que la maintenance du contrôle assure l'efficacité continue de la limitation d'une session utilisateur à l'utilisateur autorisé qui s'est connecté au système.