PSR

Rapport 2021 sur la sécurité des paiements

Livre blanc
PCI DSS v4.0

Verizon Cyber
Security Consulting

Sommaire

Avec la nouvelle version de la célèbre Norme de sécurité de l'industrie des cartes de paiement (PCI DSS), les entreprises seront mieux armées pour contrôler la sécurité des données de façon pertinente et efficace dans un monde en mutation. Il s'agit de la plus importante mise à jour depuis la toute première version publiée en 2004. Pourtant, face à la multitude d'articles et de guides qui prolifèrent sur la toile à ce sujet, vous souhaitez peut-être bénéficier d'une information claire et fiable pour en saisir tous les enjeux. Dans ce cas, le Rapport Verizon sur la sécurité des paiements (PSR) est exactement ce qu'il vous faut.

Fruit de décennies de recherches assidues, le rapport PSR vous montre le chemin pour développer une stratégie gagnante en matière de sécurité et de conformité dans l'industrie des cartes de paiement. Depuis 2010, notre rapport accompagne les équipes de sécurité de tous les niveaux : des comités de direction et de pilotage de la sécurité jusqu'aux équipes opérationnelles de protection des données et de suivi de la conformité.

À l'aide d'analyses claires et détaillées, le rapport PSR répond aux grandes questions de la sécurité des paiements :

- Comment identifier vos domaines d'action prioritaires ?
- Comment définir vos buts et vos objectifs ?
- Comment mieux déchiffrer vos besoins tout en levant les obstacles ?

Lorsqu'une entreprise est florissante, c'est généralement parce qu'elle dispose de collaborateurs productifs et motivés, qui savent parfaitement dans quelle direction avancer. Et cela vaut aussi en matière de conformité et de sécurité des données. Cette spirale vertueuse exige néanmoins un effort concerté de gestion des performances conciliant les besoins des collaborateurs comme de l'entreprise dans son ensemble.

Combien de vos salariés connaissent véritablement vos buts et objectifs de sécurité et de conformité ? Combien savent où et comment les trouver ? Quels sont vos critères pour optimiser le déploiement de vos ressources de sécurité les plus limitées ? Enfin, êtes-vous certain de prendre les bonnes décisions concernant la gestion de vos contraintes et la définition de vos buts, objectifs et stratégies ?

Bon nombre d'entreprises peinent à maintenir leur conformité PCI DSS. Pourtant, contrairement à ce qu'elles peuvent penser, cet objectif est bel et bien à leur portée. Plus encore si elles se laissent guider par les recommandations et les étapes soigneusement élaborées par Verizon dans son rapport emblématique.

Le rapport PSR a aidé d'innombrables entreprises à trouver le chemin de la réussite grâce à des programmes innovants, des modèles pratiques et des conseils inédits en matière de sécurité. En particulier, nos frameworks directement exploitables aident les professionnels de sécurité à créer et mettre en œuvre des business models et des stratégies opérationnelles robustes pour le monde de demain.

Découvrez à présent nos recommandations pour bien négocier le virage de la norme PCI DSS v4.0, qui constitue à ce jour la dixième et la plus ambitieuse de toutes les mises à jour. Verizon vous accompagne sur la voie du changement.

L'entrée en vigueur de la norme PCI DSS v4.0 promet de changer la donne pour les entreprises. C'est pourquoi vous devez prendre le temps de revoir l'ensemble des éléments concernés : des procédures aux objectifs de sécurité, en passant par les cibles, les indicateurs, les initiatives et la répartition des responsabilités.

Préparation à la norme PCI DSS v4.0

PCI DSS : repères chronologiques

PCI DSS v4.0 est la 10e version de la norme PCI. Au moment de sa publication (au mois de mars 2022), presque neuf ans se seront écoulés depuis la dernière révision majeure (version 3.0) et quatre ans depuis la dernière mise à jour en 2018 (version 3.2.1), qui n'apportait que des changements mineurs.

Avant la publication de PCI DSS v4.0, la plus longue période entre deux mises à jour avait eu lieu entre les versions 2.0 et 3.0 (parues respectivement en octobre 2010 et novembre 2013).

Historique des versions PCI DSS

Année		Version
2004	décembre	1.0
2006	septembre	1.1
2008	octobre	1.2
2009	juillet	1.2.1
2010	octobre	2.0
2013	novembre	3.0
2015	avril	3.1
2016	avril	3.2
2018	mai	3.2.1
2022	mars	v4.0

Voilà plus de 10 ans que Verizon documente les tendances de conformité dans l'univers en perpétuelle mutation de la sécurité des paiements. La série de rapports PSR suit les succès et les échecs des entreprises dans ce domaine tout en restant attentif aux avancées technologiques du secteur. Entre temps, les consommateurs comme les entreprises ont largement accru leurs activités en ligne, entraînant par là même une hausse vertigineuse du nombre de transactions par carte bancaire. Dans ce contexte, les acteurs malveillants continuent d'améliorer et d'étoffer leur arsenal en jouant habilement sur tout le répertoire des menaces (anciennes comme nouvelles) pour exploiter les failles des systèmes et processus de paiement. Parlons aussi de ces transformations digitales qui, en faisant la part belle aux technologies cloud, redessinent la physionomie du secteur de la sécurité des paiements. Un phénomène qui complique encore un peu plus la tâche des RSSI et autres responsables et professionnels de la sécurité.

La publication de la norme PCI DSS v4.0 est une réponse indispensable à ces préoccupations. Il s'agit de la révision la plus substantielle depuis la version 1.0 publiée en 2004, il y a 17 ans. Les entreprises remarqueront d'emblée la présence de changements majeurs. Si la version 4.0 n'altère pas la structure fondamentale de la norme PCI, qui inclut encore les traditionnels objectifs de contrôle et les 12 exigences clés introduites en 2006, elle y apporte toutefois des modifications importantes qui reflètent l'évolution de ces objectifs et de ces exigences. Outre de nombreuses retouches terminologiques, la nouvelle mouture met à jour d'anciennes exigences et en introduit de nouvelles dont l'entrée en vigueur sera échelonnée dans le temps.

Une question légitime subsiste : pourquoi le Conseil PCI engage-t-il une refonte de sa norme PCI DSS alors que la version 3.2 publiée en 2016 était déjà prisée pour son niveau de maturité ?

Cette mise à jour reflète les changements importants survenus dans le secteur des cartes de paiement et tient compte d'un paysage des menaces toujours plus complexe et en constante évolution. Face à l'essor des technologies, PCI DSS v4.0 trace de nouvelles orientations pour aider les entreprises à mettre en place des environnements de contrôle et de conformité efficaces dans la durée.

La version 4.0 accorde ainsi une place de choix à des technologies clés comme le cloud et l'informatique sans serveur. Pour les entreprises qui appliquent des contrôles compensatoires afin de remplir leurs exigences PCI DSS, il sera intéressant de déterminer si la nouvelle méthode de mise en œuvre personnalisée convient à leurs besoins de sécurité spécifiques.

Par ailleurs, la nouvelle norme introduit davantage de flexibilité dans la formulation des exigences, avec en prime l'ajout de déclarations d'intention. Les pages 6 et 7 de ce document explorent les deux grandes nouveautés de la version 4.0, à savoir les évaluations continues et la personnalisation des contrôles ou des environnements de contrôle.

De 2019 à la mi-2021, le Conseil des normes de sécurité PCI a examiné un nombre sans précédent de commentaires sur la version provisoire de la nouvelle norme, signe encore de son importance capitale. Pour les versions précédentes, les évaluateurs et les organisations participantes du Conseil avaient un temps limité pour faire remonter leurs commentaires. Pour la version 4.0, le Conseil a étendu cette fenêtre pour maximiser la collaboration et la participation des parties prenantes à la mise à jour de la norme PCI[1].

1 Voir l'article du Conseil des normes de sécurité PCI intitulé « PCI DSS v4.0: Anticipated Timelines and Latest Updates ».
https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates
https://www.pcisecuritystandards.org/about_us/press_releases/pr_10242019
https://www.pcisecuritystandards.org/get_involved/request_for_comments

En résumé, la mise à jour de la norme PCI DSS vise principalement à :

- Garantir la robustesse de la norme de sécurité des données face aux défis de sécurité de l'industrie des cartes de paiement
- Introduire davantage de souplesse et des méthodologies complémentaires pour une meilleure protection
- Prendre en compte les dernières avancées technologiques (systèmes de paiement, mobiles, cloud, etc.)
- Faire face à l'évolution du paysage des menaces, notamment par l'amélioration des protocoles et des méthodes de validation
- Promouvoir un processus continu d'amélioration de la sécurité et de la conformité

Chaque entreprise doit dès aujourd'hui se poser cette question essentielle :

“ Quels sont les chantiers à engager pour préparer la transition ?

Négocier la phase de transition

Attention : même si elle n'est prévue qu'en 2024, l'entrée en vigueur de la norme PCI DSS v4.0 approche à grands pas. Sa publication interviendra néanmoins dès le mois de mars 2022, ce qui laisse aux entreprises deux ans pour se mettre en conformité. Une période de transition étendue qui doit permettre aux entreprises de digérer les nombreux ajouts de la nouvelle mouture. Dans cette optique, la version 3.2.1 restera active pendant 18 mois après la publication de l'ensemble des documents relatifs à PCI DSS v4.0. À la fin de cette période de transition, la version 3.2.1 tirera sa révérence pour laisser la place à la version v4.0 qui demeurera l'unique version en vigueur. Outre cette période de 18 mois qui verra coexister les versions 3.2.1 et v4.0, une fenêtre supplémentaire sera prévue pour l'introduction de nouvelles exigences dites « future dated », lesquelles ne deviendront obligatoires qu'à partir de 2025.

Certaines entreprises estiment peut-être disposer d'un temps amplement suffisant pour améliorer leurs contrôles et mettre à niveau leurs environnements de conformité. Pourtant, vu l'étendue des modifications à venir (comme l'approche de mise en œuvre personnalisée) il n'est jamais trop tôt pour commencer à se préparer.

Aligner ses objectifs pour mieux protéger ses données

Le Conseil des normes de sécurité PCI a élaboré ses exigences pour aider les entreprises à instaurer de bonnes pratiques de sécurité. L'esprit de la norme PCI DSS est clair : encourager les entreprises à concevoir, hiérarchiser, mettre en œuvre et maintenir des objectifs conformes qui aboutiront à un environnement de contrôle efficace et pérenne. Cette visée apparaît sans doute de façon plus explicite aujourd'hui que dans les précédentes versions de la norme PCI.

Dix-huit ans après la publication de la version 1.0 en 2004, la plupart des entreprises peinent toujours à protéger efficacement et durablement les données de carte de paiement. Celles qui parviennent à satisfaire l'ensemble des exigences dans la durée – au lieu de remédier aux problèmes au cas par cas dans l'unique but de valider l'audit annuel – déploient une stratégie fondée sur des objectifs durables et réfléchis. Une fois leurs objectifs tirés au clair, il devient plus facile pour elles de déployer des processus de contrôle et de validation personnalisés.

Fortes de ce savoir, certaines entreprises parviennent à bâtir une culture qui accorde toute sa place à la sécurité. Malheureusement, notre état des lieux de la conformité réalisé dans le cadre du rapport PSR 2020 met au jour un fait assez préoccupant : pour presque trois quarts des entreprises (72,1 %), la norme PCI DSS apparaissait comme un simple audit à valider, et non comme l'occasion de créer des environnements de contrôle vraiment efficaces et durables. Certes, des erreurs de contrôle peuvent encore survenir au sein d'organisations dotées d'environnements performants. Ces dysfonctionnements restent pourtant très brefs car ils sont rapidement détectés et corrigés. Cela nécessite néanmoins des capacités qui font défaut aux environnements de contrôle de la plupart des entreprises.

La norme PCI DSS v4.0 met davantage l'accent sur cette transition vers la sécurité en tant que culture d'entreprise, y compris sur la collecte accrue d'informations de validation dans la durée pour encourager le déploiement de processus de sécurité continue.

Développer des solutions pérennes de conception des contrôles

L'absence d'objectifs clairs et d'un plan de défense stratégique précis conduit à la conception de dispositifs de sécurité plus lâches. Les RSSI et les responsables de la sécurité doivent prendre le temps de réfléchir aux besoins spécifiques de leur organisation et aux solutions à apporter aux différents problèmes, plutôt que de se précipiter dans la mise en œuvre des nouvelles exigences. Qu'elle soit ancienne ou nouvelle, chaque exigence de la norme doit faire l'objet d'un examen attentif. Les chefs de projet doivent se garder d'assigner des tâches avant de comprendre la portée du projet en question, c'est-à-dire ses objectifs et ses contraintes.

Trop souvent, l'importance d'une bonne solution de conformité et de sécurité des données est reléguée au second plan, tandis que les planificateurs et les professionnels de la sécurité se démènent pour faire face au manque de personnel et à une pléthore d'alertes par e-mail. Certains projets annuels de validation de la conformité sont perçus comme couronnés de succès simplement parce qu'ils ont permis de mettre en place quelques contrôles manquants en vue de recevoir le très convoité rapport final de conformité DSS, le fameux « RoC ». Une telle approche trahit pourtant l'esprit de la norme PCI DSS.

Améliorer les méthodes et procédures de validation

Parmi les principaux changements de la version 4.0 figurent des méthodes et procédures de validation améliorées, qui peuvent désormais être mises en œuvre dans le cadre d'une approche personnalisée fondée sur des objectifs. À l'occasion des réunions communautaires de 2019, le Conseil des normes de sécurité PCI a fait part de son intention d'introduire ces méthodes et procédures de validation améliorées dans la version 4.0.

L'approche définie est la méthode classique qui consiste à déployer les contrôles de sécurité requis dès lors qu'ils sont nécessaires. La version 4.0 ne mettra pas fin à cette méthode traditionnelle de validation du standard PCI DSS. Avec l'approche définie, les exigences sont satisfaites et validées selon un cahier des charges très spécifique, parfois indépendamment des résultats concrets du contrôle (c'est-à-dire sans prêter attention à son efficacité dans la durée). Mais dans le cadre de l'approche personnalisée, les entreprises peuvent employer des méthodes qui diffèrent des exigences PCI DSS traditionnelles, tant qu'elles peuvent démontrer que les contrôles sont efficaces et répondent à l'intention des exigences en question.

Lors d'un audit de conformité PCI DSS, les entreprises peuvent choisir l'une ou l'autre des approches, voire les deux, pour l'ensemble des exigences clés. Autrement dit, la norme PCI DSS v4.0 autorise une approche hybride : les entreprises peuvent suivre l'approche définie pour certaines exigences, et l'approche personnalisées pour d'autres. Les deux approches peuvent même coexister au sein d'une seule et même exigence tant que l'entreprise parvient à atteindre l'objectif de sécurité visé. Gardez cependant à l'esprit que l'approche personnalisée est formellement interdite pour certaines exigences.

Approche définie vs approche personnalisée

L'approche définie

Créée en même temps que la norme PCI, l'approche définie est la méthode traditionnelle en matière de contrôle de sécurité et de validation de la conformité. Il s'agit d'un ensemble d'exigences, de contrôles et de procédures de tests à caractère prescriptif. La norme PCI décrit d'ailleurs plus en détail ces contrôles et la manière dont ces procédures de tests de validation doivent être mises en place.

L'« approche définie » désigne donc le fait pour les entreprises de s'en tenir aux exigences et procédures de test (traditionnelles) telles qu'elles figurent dans la norme PCI DSS. Cette approche reste valide dans la mesure où les entreprises bénéficient toujours de la présence de lignes directrices sur la manière d'atteindre leurs objectifs. Bon nombre d'entre elles ne verront aucune utilité à suivre l'approche personnalisée pour atteindre les objectifs de contrôle.

L'approche personnalisée

Avec l'approche personnalisée, place au sur mesure : les entreprises peuvent personnaliser leurs contrôles de sécurité voire adopter des contrôles qui ne figurent pas dans la norme. Cette nouvelle approche de validation des contrôles PCI DSS met en place une obligation de résultat et non de moyens. Comme déjà évoqué, les contrôles personnalisés doivent nécessairement remplir l'objectif de sécurité associé à une exigence.

L'approche personnalisée requiert généralement des efforts supplémentaires pour constituer un dossier :

Conception des contrôles et justification de leur adéquation aux objectifs et aux intentions définis dans la norme

- Test des contrôles en interne
- Risques liés aux contrôles
- Performances des contrôles
- Efficacité des contrôles
- Maintenance des contrôles
- Procédures de test externes pour valider la conformité des contrôles

Dans la version 4.0, les exigences et les options de validation ont été remaniées pour mettre l'accent sur les objectifs de sécurité tout en laissant aux entreprises une marge de manœuvre dans la méthode à suivre pour respecter l'intention des exigences. La norme PCI inclut des déclarations d'intention qui décrivent les résultats de sécurité à atteindre dans le cadre d'une approche personnalisée. Ces déclarations précisent et clarifient les résultats attendus tout en introduisant davantage de flexibilité dans la manière de les atteindre.

Grâce à cette approche, les entreprises peuvent prendre les devants et déployer des solutions et des technologies de sécurité innovantes, même si elles n'ont pas encore été prévues par la norme PCI DSS. Les méthodes de validation se concentrent davantage sur des résultats de sécurité spécifiques, ce qui laisse aux organisations la possibilité de prouver l'efficacité de leurs propres méthodes pour atteindre les résultats de sécurité escomptés.

Cette nouvelle approche permet ainsi aux entreprises de concevoir et développer leurs propres contrôles de sécurité en suivant ces étapes :

- Déterminer les contrôles qui répondent à un objectif de sécurité donné
- Soumettre un dossier détaillé à l'auditeur de sécurité qualifié (QSA, Qualified Security Assessor), en présentant l'approche choisie et en démontrant son efficacité
- Après un examen attentif des pièces justificatives, l'évaluateur valide ou non l'efficacité du contrôle

Conséquences de l'approche personnalisée

La personnalisation des contrôles de sécurité doit suivre un cadre très structuré afin d'obtenir des résultats mesurables et prévisibles. Les entreprises qui disposent d'environnements de contrôle matures seront plus confiantes pour aborder la nouvelle approche de validation personnalisée. Elles devraient aussi avoir moins de difficultés à réécrire des procédures de tests pour valider la conformité de leurs systèmes aux dernières exigences PCI DSS.

Cette nouvelle méthode de validation nécessitera sans doute, du moins au début, une charge de travail supplémentaire. Et pour cause, les entreprises devront constituer un dossier, concevoir des contrôles et préparer des évaluations et des diagnostics des risques qui devront être ensuite examinés par le QSA.

Même si cette approche laisse aux entreprises une plus grande latitude dans la réalisation des 12 exigences clés, la norme formule explicitement le besoin pour chaque dispositif personnalisé de respecter l'intention et les objectifs de contrôle liés à ces exigences.

En ce sens, l'approche personnalisée requiert l'adoption d'une méthode fiable pour la conception et la gestion des contrôles de sécurité, mais aussi pour la maintenance de l'environnement de contrôle. Elle exige davantage de maturité en termes de processus et de capacités : de la conception à la mise en œuvre et au suivi des contrôles, en passant par l'évaluation des risques associés.

Aux entreprises qui opteraient pour l'approche personnalisée sans toutefois disposer d'un environnement de contrôle robuste soutenu par des processus et des capacités de gestion de la conformité raisonnablement matures, nous conseillons de gagner d'abord en maturité et d'implémenter les changements étape par étape. Elles s'épargneront ainsi la refonte de leur environnement de contrôle, avec toutes les conséquences inattendues qui peuvent en découler.

En concertation avec le QSA ou l'évaluateur de sécurité interne (ISA), les entreprises doivent convenir de procédures de test à développer. Mais même en prenant toutes les précautions, le risque de conséquences inattendues liées à la conception et à la mise en œuvre de contrôles personnalisés reste bel et bien réel. Les entreprises doivent identifier les zones d'ombre et chercher des relations de cause à effet entre les contrôles, les systèmes et l'environnement.

La possibilité pour les organisations de concevoir et déployer leurs propres contrôles, tout en respectant l'intention des exigences, peut être source de nouveaux risques. C'est pourquoi les entreprises doivent comprendre les implications d'une telle approche, notamment les responsabilités supplémentaires qu'elle nécessite. Elles doivent déterminer leurs capacités et compétences dans différents domaines – conception, mise en œuvre, maintenance et suivi des contrôles personnalisés – ainsi que leur aptitude à remplir toutes les exigences liées aux méthodes choisies. Vous l'aurez compris, cette nouvelle approche conviendra surtout aux entreprises dont les processus de sécurité, de conformité et d'évaluation des risques ont déjà atteint une certaine maturité.

Pour en savoir plus sur la notion de maturité et les indicateurs à prendre en compte, consultez les pages 21 à 29 du Rapport Verizon 2019 sur la sécurité des paiements.

Conséquences inattendues : de quoi parle-t-on au juste ?

Le concept de « conséquences inattendues » a été popularisé par le sociologue Robert K. Merton qui l'utilise pour décrire les résultats imprévus d'une action délibérée. Dans son article fondateur « The Unanticipated Consequences of Purposive Social Action », le sociologue américain distingue trois types de conséquences inattendues :

- **Avantages fortuits :** des retombées positives inattendues (on parle parfois d'aubaine ou de sérendipité)
- **Inconvénients fortuits :** une conséquence négative qui entraîne des retombées positives
- **Effets pervers :** une conséquence négative sans retombées positives[2]

2 « Unintended consequences », Wikipedia. https://en.wikipedia.org/wiki/Unintended_consequences

Risques associés aux contrôles : l'incident de l'Ever Given

En matière de conception de sécurité, sous-estimer les conséquences inattendues peut se révéler très dangereux. Pourtant, bon nombre d'entreprises continuent de négliger ce risque. Même d'infimes retouches apportées à des systèmes complexes peuvent générer des résultats imprévus. Si la planification et l'anticipation de l'ensemble des répercussions possibles sont essentielles lors de la conception, des interdépendances complexes peuvent entraver les prévisions. La sécurité des paiements requiert une stratégie de conception complète et soigneusement documentée pour écarter tout imprévu potentiellement dommageable. C'est particulièrement vrai lorsqu'on combine l'approche personnalisée aux technologies phares de la transformation digitale : 5G, paiement sans contact, blockchains, intelligence artificielle ou machine learning.

La catastrophe de l'Ever Given, ce porte-conteneurs échoué dans le canal de Suez en mars 2021, illustre bien la manière dont un défaut d'anticipation et de coordination dans la conception, la stratégie et la planification peut aboutir à un fiasco. La concomitance de plusieurs facteurs a abouti au blocage du porte-conteneurs pendant plus de six jours :

1 **Alors que les porte-conteneurs ont au moins doublé de taille depuis l'année 2000, notamment en largeur, les réglementations et la coordination entre le secteur des transports maritimes et les responsables du canal de Suez sont, elles, restées limitées[3].**

2 **Lors de l'incident, l'Ever Given (l'un des plus longs navires en service) s'était échoué en travers de la section étroite du canal, qui, contrairement à d'autres segments, n'avait pas été élargie lors du projet de réaménagement égyptien de 2015.**

3 **L'hydrodynamique d'un large porte-conteneurs dans un canal étroit et peu profond réduit les marges de manœuvre, accroissant ainsi les phénomènes de squat et de berge qui compliquent le pilotage[4]. Des vents forts et une tempête de sable observés le jour de l'incident auraient aggravé la perte de contrôle.**

> **« Les plans les mieux conçus des souris et des hommes vont souvent de travers »**
>
> — Robert Burns[5]

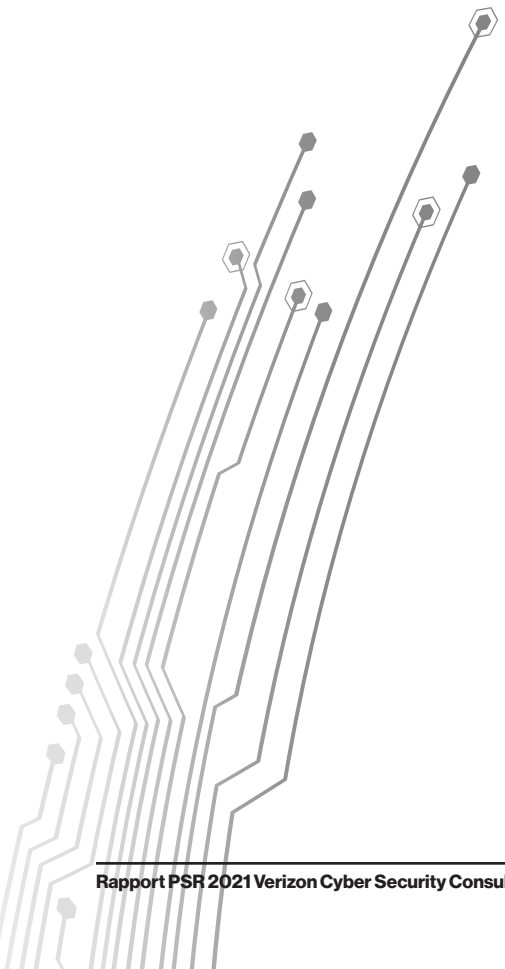
Concernant l'implémentation des changements de conception, les RSSI et responsables de sécurité doivent tenir compte du « principe de précaution »[6], lequel exige de prouver non pas la présence, mais l'absence de tout préjudice. Une approche souvent plébiscitée par les décideurs politiques lorsqu'ils doivent prendre des décisions ou effectuer des remaniements en l'absence de données probantes.

D'après un article du blog Farnam Street, « le principe de précaution nous oblige à poser de nombreuses questions difficiles sur la nature du risque, sur les concepts d'incertitude et de probabilité, ou encore sur le rôle du gouvernement et l'éthique. Il nous invite aussi à interroger nos intuitions quant à la meilleure décision à prendre dans une situation donnée »[7]. Lorsqu'elles planifient la modification de leurs environnements, ces considérations peuvent aider les entreprises à se prémunir contre des compromissions de données onéreuses.

3 « The Impact of Mega-Ships », Organisation de coopération et de développement économiques (OCDE), Forum international du transport, 2015. https://www.itf-oecd.org/sites/default/files/docs/15cspa_mega-ships.pdf
4 Marc Vantorre et al., « Maneuvering in Shallow and Confined Water », Encyclopedia of Maritime and Offshore Engineering, 20 avril 2017 https://doi.org/10.1002/9781118476406.emoe006,
5 « To a Mouse », Wikipédia, https://sco.wikipedia.org/wiki/To_a_Mouse
6 « Principe de précaution », Wikipédia, https://fr.wikipedia.org/wiki/Principe_de_précaution
7 « The Precautionary Principle: Better Safe than Sorry? » Farnam Street, juin 2021. fs.blog/2021/06/precautionary-principle

Modèle « objectifs, exigences et contraintes » : une approche pour résoudre des problèmes complexes

Une conception pérenne passe par une stratégie solide et un business model fiable. Avec la norme PCI DSS v4.0 et la conception de contrôle personnalisée, les RSSI et autres responsables doivent clairement cerner la portée de chaque projet – c'est-à-dire ses objectifs et ses contraintes – relatif aux exigences. Afin d'aider les entreprises à résoudre les problèmes les plus complexes, Verizon a développé le modèle « objectifs, exigences et contraintes », essentiel pour concevoir des environnements personnalisés à la fois efficaces et durables. Nous vous présentons ce modèle de façon détaillée dans le rapport PSR 2022.



Appliquer une pensée logique

La majorité des entreprises conçoivent et mettent en œuvre des environnements de contrôle qui ne sont ni vraiment efficaces, ni vraiment durables. Pourquoi est-ce si important de créer une méthode ou un processus de conception éprouvés ? La réponse est simple : une telle méthode vous donne toutes les chances de créer des produits et services qui feront leurs preuves dans la durée. Les dentistes, par exemple, suivent une série d'étapes infaillibles lorsqu'ils réalisent un soin. Les maçons, eux, ont une méthode sûre pour préparer le terrain et poser les fondations d'une maison. Dès lors, pourquoi en irait-il autrement pour les professionnels de sécurité qui conçoivent des contrôles en matière de protection des données ? Bon nombre d'entreprises manquent non seulement d'une méthode logique pour simplifier la définition des buts et des objectifs, mais aussi des capacités indispensables à leur réalisation. L'application d'une pensée logique améliore la capacité à réaliser des progrès de façon incrémentielle au moyen d'étapes claires et prévisibles.

De fait, l'incident de l'Ever Given s'explique autant par un manque d'anticipation que par une mauvaise prise en compte des objectifs stratégiques, des exigences réglementaires et des contraintes. Les responsables de sécurité ont tout à gagner à considérer ce modèle triangulaire et interconnecté pour éviter les oublis pendant la phase de conception.

Lors des audits de conformité, les conversations entre le QSA et ses clients visent souvent à justifier le véritable statut d'une exigence PCI DSS. Généralement, un QSA part du contrôle tel qu'il se présente au moment de l'audit pour remonter jusqu'aux décisions et actions (prises ou non) qui ont contribué de façon directe ou indirecte au résultat négatif. Inévitablement, les conversations reviennent à un moment ou un autre sur les objectifs de sécurité et de conformité de l'entreprise. Dans la majorité des cas, les preuves relatives à la gestion de l'environnement de contrôle trahissent une certaine négligence à l'égard des objectifs, exigences et contraintes. Une négligence qui, en définitive, aboutit à des erreurs de contrôle.

Cette situation s'explique la plupart du temps par des insuffisances en matière de conception, de mise en œuvre et de maintenance qui affaiblissent l'efficacité du système. Or, chaque contrôle PCI DSS opère systématiquement au sein d'un tel système. La présence d'un contrôle défaillant tient souvent à une évaluation trop superficielle de sa fiabilité et de sa résilience en regard des autres contrôles avec lesquels il entretient une dépendance. En outre, ces contrôles comptent rarement avec l'appui opérationnel d'un environnement pérenne, ce qui affecte considérablement leur efficacité.

Qu'est-ce qu'un objectif ?

Les objectifs sont des résultats spécifiques, quantifiables et mesurables que votre entreprise se propose d'atteindre dans le cadre de sa mission. Vous pouvez quantifier à l'avance vos objectifs de sécurité et de conformité. Et leur réalisation (ou non-réalisation) doit être mesurée de façon spécifique tout au long du déploiement et de l'exécution des tâches et processus qui leur correspondent.

Une communication claire au sujet des objectifs permet à vos collaborateurs de donner du sens à leurs tâches quotidiennes. Elle favorise aussi un plus grand sens du devoir, chacun se sentant responsable vis-à-vis de l'ensemble de l'équipe. Ce n'est pas tout, une bonne communication jette aussi les bases d'une collaboration fructueuse allant vers la réalisation des objectifs annoncés.

Enfin, voici quatre façons dont des objectifs clairs en matière de sécurité et de conformité PCI DSS peuvent améliorer les performances de vos collaborateurs :

- Des objectifs clairs orientent les efforts vers les activités liées aux objectifs
- Ils dynamisent les collaborateurs et les poussent à s'investir plus pleinement
- Ils les encouragent à mobiliser leurs connaissances ou à acquérir de nouvelles compétences
- Des rappels fréquents sont facteurs de persévérance et peuvent se traduire par un redoublement d'efforts pour atteindre des objectifs ambitieux

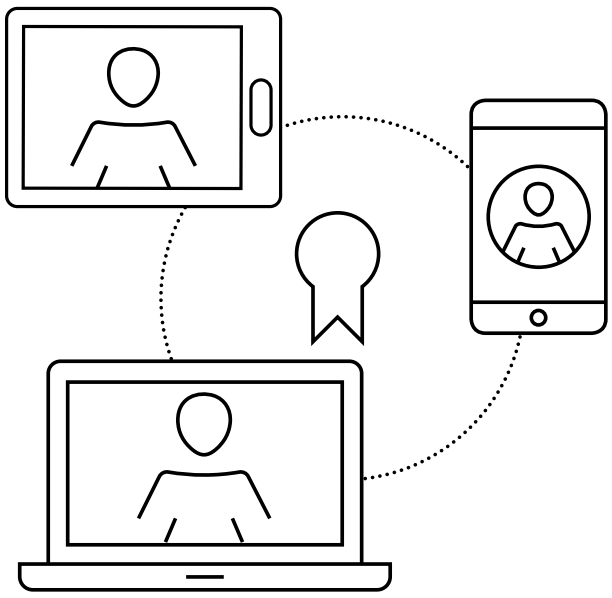
Il convient donc de se poser les questions suivantes :

- Quels objectifs de conformité et de sécurité des données ont été fixés et communiqués au sein de l'entreprise ?
- S'agit-il des mêmes objectifs que ceux visés par les membres de chacune des 4 lignes de maîtrise (cf. page 12 du rapport PSR 2019) ? Faut-il leur demander quels sont les objectifs de sécurité et de conformité prioritaires ?
- Au sein de l'environnement de contrôle, quel est le pourcentage de contrôles PCI DSS véritablement efficaces et pérennes ?
- Quelle part du succès relève d'une bonne conception plutôt que du hasard ?

Établir des liens entre les objectifs fixés et des contrôles insuffisamment pérennes et efficaces devrait aller de soi. C'est pourtant loin d'être le cas dans de nombreuses entreprises. Mettre au jour de tels liens ne devrait pas exiger des compétences d'analyse très poussées. Il est peu probable que les entreprises atteignent un objectif qu'elles ne se sont pas fixé. Ceci dit, très peu d'entreprises se donnent explicitement pour objectif de mettre en place des contrôles de sécurité efficaces et pérennes au sein de leur environnement. Comme déjà évoqué à plusieurs reprises, il est impératif que vous atteigniez votre cible – c'est-à-dire des résultats prévisibles, cohérents et reproductibles – grâce à une conception avisée, et non par hasard.

Faute d'objectifs clairement définis, vos équipes de sécurité et de conformité auront toutes les chances de stagner : elles peineront à obtenir les investissements nécessaires et, partant, n'obtiendront que de maigres résultats.

Les RSSI et leurs équipes de sécurité ont du pain sur la planche. Cela ne fait aucun doute. Dans ce contexte, les opérations de routine soi-disant plus urgentes prennent toujours le pas sur les tâches d'autocritique et de préparation à l'avenir (Verizon traite ce sujet de façon approfondie dans son rapport PSR 2020). Définir adéquatement vos objectifs de conformité et de sécurité des données, c'est donner une vision claire à l'ensemble des collaborateurs impliqués de près ou de loin dans la gestion et la sécurité de votre environnement de contrôle, y compris dans vos 4 lignes de maîtrise.



La théorie des contraintes appliquée à la sécurité des paiements

La théorie des contraintes (de l'anglais Theory of Constraints, ou TOC) est une méthodologie éprouvée de gestion des processus. Elle permet aux entreprises de détecter et d'agir sur les causes profondes qui entravent l'efficacité et la pérennité de leurs environnements de contrôle. Elle définit d'abord un ensemble d'étapes pour identifier la principale contrainte à l'atteinte d'un objectif. Elle se concentre ensuite sur les moyens d'éliminer ou d'atténuer ce facteur limitant pour qu'il n'agisse plus comme un obstacle ou une contrainte.

Selon la théorie des contraintes, la capacité d'un système à atteindre ses objectifs est toujours limitée par une poignée de facteurs limitants. La théorie vise donc à améliorer ces systèmes selon une approche scientifique. Eliyahu M. Goldratt, le père de cette théorie, la décrit comme « un processus d'amélioration continue » et un mode de pensée qui permet à chacun d'apporter des solutions simples à des problèmes complexes[8].

Tout système complexe – y compris en matière de conformité PCI DSS et de sécurité des données en général – consiste en une série d'activités interconnectées. Le principe est le suivant : au moins une de ces activités agit comme une contrainte sur l'ensemble du système, et ce dernier sera toujours soumis au minimum à une contrainte. Parfois, c'est le processus tout entier qui représente la contrainte. Dans d'autres cas, il peut s'agir d'un département de l'entreprise, voire même de sa direction. En identifiant la ou les activités qui constituent le maillon faible du système, il devient possible de prendre des mesures correctives afin qu'elles ne soient plus un frein. Vous déplacez alors le facteur limitant, qui vient se loger dans une autre partie du système ou dans un élément externe à celui-ci. Cette méthodologie a toute sa place dans le domaine de la conformité PCI DSS, où elle permet de lever les freins qui empêchent les environnements de contrôle d'atteindre les niveaux d'efficacité et de pérennité requis.

L'importance d'une vue d'ensemble

Plus qu'une méthode de définition des priorités, la théorie des contraintes permet d'analyser un système complexe pour identifier, mettre en cause et corriger les suppositions infondées. Vous pouvez ainsi passer en revue chaque étape ou procédure dans le contexte plus général d'un processus, d'un département ou de l'entreprise. Cette théorie adopte une approche résolument holistique dans la mesure où elle envisage les entreprises comme une chaîne de départements ou de fonctions.

Ces entreprises sont dotées de nombreux chaînons mouvants. La théorie des contraintes vous aide à identifier la méthode la plus efficace pour atteindre votre objectif tout en maîtrisant vos dépenses. Grâce à des outils spécifiques, elle trace une voie claire et cohérente pour reconnaître et résoudre des problèmes sans jamais perdre de vue les objectifs de l'entreprise.

La théorie des contraintes offre un cadre d'amélioration continue qui vise à maximiser l'impact des changements. Non seulement cette démarche holistique d'identification des contraintes vous donne plus de contrôle sur vos processus, mais elle révèle aussi la présence de capacités inexploitées qui, bien souvent, sont mobilisables sans investissement supplémentaire. Autrement dit, la théorie des contraintes s'inscrit en faux contre la tendance à investir systématiquement dans de nouveaux équipements et vous encourage au contraire à optimiser vos ressources existantes. Une solution idéale pour bon nombre d'entreprises qui doivent renforcer leur conformité PCI. (Le rapport PSR 2022 revient en détail sur la façon d'appliquer la théorie des contraintes aux programmes de sécurité.)

8 Eliyahu M. Goldratt, « What is this thing called Theory of Constraints and how should it be implemented? », The North River Press, 1999.

La Théorie des contraintes vous aide à répondre de façon plus satisfaisante à ces questions élémentaires :

- Pourquoi changer ? (Quel est l'objectif ?)
- Qu'est-ce qui devrait changer ? (Où est le problème et quelle en est la cause profonde ?)
- Quel est l'objectif à atteindre ? (Quelle est la solution ?)
- Comment mettre en place le changement ? (Comment assurer sa mise en œuvre ?)

Il s'agit d'une puissante approche pour :

- Clarifier vos buts, vos objectifs et vos exigences
- Déterminer les facteurs critiques de réussite (entre trois et cinq pour chaque objectif)
- Mettre en exergue les variables et les conditions nécessaires pour que le système atteigne les objectifs
- Identifier les conditions nécessaires à chaque facteur critique de réussite[9]

Les concepts de « conditions nécessaires » et « conditions suffisantes » aident à rendre compte des diverses relations entre les contrôles de sécurité PCI DSS, leurs différents états et la manière dont ils sont liés les uns aux autres. Ils sont également utiles pour décrire les relations entre les contrôles internes et externes à la norme PCI DSS, et ce, afin d'atteindre les niveaux requis d'efficacité et de pérennité des contrôles. Ce dernier point aura toute son importance pour les organisations qui choisissent l'approche personnalisée de conception et de validation.

9 H. William Dettmer, « The Logical Thinking Process: A Systems Approach to Complex Problem Solving », American Society for Quality Press, 2007.

PCI DSS v4.0 : huit conseils pour bien négocier le virage

1. N'attendez pas

Les entreprises ne doivent pas repousser leurs préparatifs au motif que la version 4.0 de la norme PCI DSS n'est pas encore entrée en vigueur. Même si votre entreprise est en parfaite conformité avec la version 3.2.1., ce serait une erreur de penser que vous avez le temps.

2. Prenez un bon départ : conformez-vous à la version 3.2.1

Mettez toutes les chances de votre côté, et ce dès le début. Déterminez dans quelle mesure votre entreprise adhère ou non à l'approche définie pour chaque exigence applicable à vos données de titulaires de carte. Évaluez la fiabilité et la résilience de vos systèmes de contrôle. Améliorez votre vitesse de détection et de correction des contrôles défaillants. Vérifiez si chacune des exigences remplit véritablement l'objectif de sécurité énoncé qui lui est associé.

3. Dressez la liste des exigences du PCI DSS v4.0

Passez soigneusement en revue toutes les exigences de la norme PCI DSS v4.0 en prenant note des évolutions : contrôles modifiés, supprimés, ajoutés, renumérotés, ou obligatoires à partir d'une certaine date. Assurez-vous de bien comprendre l'intention et l'objectif de contrôle relatifs à chaque exigence dans le cadre de la norme PCI DSS. Les principales transformations concernent les exigences clés n° 12, 11, 10 et 8 (par ordre d'impact croissant).

4. Choisissez minutieusement votre approche de conception et de validation des contrôles

Le choix de l'approche personnalisée peut, dans un premier temps, se traduire par une charge de travail supplémentaire pour préparer vos contrôles de sécurité sur mesure aux audits de conformité. Bien que cette approche puisse augmenter les risques associés aux contrôles, elle offre toutefois une solution plus fiable et stable que l'approche définie qui, dans le cadre des contrôles compensatoires, requiert de justifier une contrainte opérationnelle ou technique. (Pour des exemples sur la façon de mesurer l'efficacité des contrôles, voir les pages 23 et 41 du rapport PSR 2018.) À l'instar des contrôles traditionnels, les contrôles personnalisés doivent prouver leur efficacité dans la durée afin de satisfaire sans interruption l'intention et l'objectif de contrôle d'une exigence.

5. Définissez votre approche personnalisée avec le plus grand soin

Si vous choisissez l'approche personnalisée pour tout ou partie de votre environnement, vous devez vous préparer à la charge de travail que celle-ci implique. La conception des contrôles doit en effet répondre à des impératifs d'efficacité et de pérennité au sein de leur environnement. Vous devrez également conserver des preuves documentées pour démontrer l'adéquation de vos contrôles avec l'intention de l'objectif ou des objectifs de sécurité correspondants. L'approche personnalisée requiert donc une méthode de documentation précise et structurée. Pour évaluer l'efficacité du contrôle en interne avant sa validation externe, on fera donc appel à un collaborateur chevronné qui s'appuiera sur le triptyque compétence, maturité et tests. Ce travail est indispensable pour atteindre le but ultime : valider et approuver vos contrôles.

6. Utilisez des modèles de conception et de gestion des contrôles

De toute évidence, il est essentiel d'évaluer régulièrement l'efficacité des contrôles. Ici, la création d'une documentation structurée, certes chronophage, s'avèrera extrêmement utile. L'élaboration et l'application cohérentes d'un modèle standardisé, qui génère un profil de conception pour chaque contrôle de sécurité ou système de contrôle requis, est une bonne pratique recommandable à toutes les organisations, surtout lorsqu'elles optent pour une approche de contrôle personnalisée. (Pour plus d'informations à ce sujet, voir la section « Conception des contrôles : nécessité et valeur des modèles » à la page 16.)

7. Validez la conception des contrôles en amont

Durant la phase de conception des contrôles, vous devez partager vos ébauches avec les évaluateurs (ISA et QSA) le plus tôt possible afin de déterminer leur adéquation aux exigences et objectifs de sécurité correspondants. Notez que l'absence de documentation rigoureuse sur les tenants et les aboutissants de vos contrôles personnalisés (conception, exécution, maintenance, évaluation) peut retarder l'approbation des évaluateurs.

8. Préparez-vous à des évaluations continues

Définissez les exigences et les contraintes applicables à votre équipe de sécurité pour faciliter la conception, la mise en œuvre et la maintenance des évaluations continues. Pour ce faire, vous devez planifier vos capacités et obtenir le soutien de vos équipes pour qu'elles évaluent, documentent et rendent compte fréquemment de l'état de l'environnement de contrôle tout au long de l'année. La collecte de preuves de conformité au regard de la norme PCI DSS doit devenir une activité routinière au sein de votre entreprise.

Conception des contrôles : nécessité et valeur des modèles

Les modèles de conception présentent des avantages substantiels pour l'amélioration des systèmes, notamment parce qu'ils sont gages de simplicité, de transparence et de cohérence dans le déploiement, l'exploitation et la maintenance des contrôles. Les modèles facilitent également la détection précoce des problèmes dans la conception et l'exécution des contrôles en question. Enfin ils contribuent à l'efficacité et à la solidité de l'environnement en fournissant une perspective indispensable sur l'objectif, la fonction et les limites opérationnelles du contrôle concerné.

En général, un document de présentation PCI DSS doit être préparé pour chaque système de contrôle et indiquer pour chacun d'eux les 12 éléments suivants :

1. **Objectif :** définit le ou les objectifs applicables au contrôle ou au système de contrôle
2. **Responsable :** désigne un référent et définit le partage des responsabilités
3. **Fonction :** décrit la fonction du contrôle (gestion, procédure, technique, etc.)
4. **Type de contrôle :** précise la nature du contrôle (prévention, détection, correction ou pilotage)
5. **Architecture :** dépeint l'architecture du contrôle (propre au système, classique ou hybride...)
6. **Risques associés :** souligne les principaux risques ciblés par le contrôle, ainsi que la méthode utilisée (matrice de risques et contrôles, mapping...)
7. **Procédures de test :** décrit ou énumère des procédures et standards de tests de contrôle
8. **Mise en œuvre :** spécifie le champ d'application, le contrôle, la mise en œuvre de la procédure et les dépendances, en énumérant le contrôle PCI DSS primaire et tous les contrôles PCI DSS subsidiaires
9. **Exécution :** documente les spécifications des opérations de contrôle et définit les processus du périmètre, les dépendances opérationnelles, les processus annexes et les exigences additionnelles du contrôle, ainsi que les impacts des composants sur les personnes, les systèmes, les processus et les tiers
10. **Maintenance :** définit les spécifications et les processus de maintenance des contrôles, ainsi que leur portée
11. **Indicateurs de performance :** fournit une liste de KPI et d'autres indicateurs PCI DSS permettant de mesurer les performances des contrôles
12. **Gouvernance :** liste les politiques, standards, dispositifs et réglementations connexes[1.0]

10 Pour plus d'informations sur la documentation liée aux profils de contrôle, voir le Rapport Verizon 2018 sur la sécurité des paiements (page 12), https://enterprise.verizon.com/resources/reports/2018/2018_payment_security_report_en_xg.pdf

Rapport PSR 2021 Verizon Cyber Security Consulting
Le point sur la norme PCI DSS v4.0

Version originale publiée le 4 novembre 2021

Rédaction

Auteur principal
Ciske van Oosten

Coautrice
Cynthia B. Hanson

Éditrice principale
Cynthia B. Hanson

Contributeurs
Abdelkrim Aoued Ahmed Bacha, Claire Lavelle, John Galt, Michelle Wire, Mikhail Banguerski, Sean Sweeney

Pôle conseil PCI et sécurité des paiements

Responsable de la sécurité Verizon Cyber Security Consulting
Kristof Philipsen

Responsable mondial
Sam Junkin

Région Amériques
Matthew Arntsen

Région APAC
Ferdinand Delos Santos

Région EMEA
Loic Breat

Business intelligence
Ciske van Oosten

Adresse e-mail de l'équipe
paymentsecurity@verizon.com

Les profils de conception peuvent avoir un impact positif sur la qualité des contrôles et de leur environnement. Des spécifications claires sur la conception et le fonctionnement des contrôles permettent en effet de mieux cerner les performances attendues. Elles clarifient aussi les limites de la conception et énumèrent les exigences de fonctionnement et de maintenance des principaux systèmes de contrôle. Ces profils donnent donc aux équipes de sécurité et de conformité toutes les indications nécessaires pour détecter et corriger les écarts en amont et éviter ainsi les éventuelles erreurs de contrôle. En règle générale, plus les profils de conception sont détaillés, plus les contrôles sont fiables et plus les performances sont prévisibles.

Pour résumer, le processus de conception a pour finalité de garantir l'efficacité des contrôles en agissant sur ces quatre axes : la cohérence, l'exhaustivité, la fiabilité et la rapidité.

Les points à retenir

La conception des contrôles requiert une méthode systématique. La norme PCI DSS définit un ensemble de contrôles dépendants et interdépendants qui ne sont véritablement efficaces et pérennes qu'une fois adaptés à l'environnement spécifique d'une entreprise. Sans une méthode délibérée et systématique de conception, la fiabilité de chaque contrôle dépend surtout de la motivation de l'équipe ou de la personne chargée de sa mise en œuvre, et ne reflète nullement la qualité de la conception en matière d'efficacité ou de durabilité.

Des lacunes se nichent généralement au niveau des dépendances. Voilà un point sur lequel on ne saurait trop insister. Les organisations qui déploient des contrôles PCI DSS prêts à l'emploi rencontrent des problèmes bien connus. La raison ? Leurs collaborateurs partent du principe que les contrôles fonctionnent correctement et n'ont besoin d'aucune retouche. Il faut souvent que les choses tournent mal pour que les organisations se penchent réellement sur la conception des contrôles et mettent en œuvre des processus subsidiaires pour s'assurer que ces contrôles fonctionnent comme prévu et de manière durable.

Lorsqu'ils procèdent à un audit de conformité, les QSA sont souvent surpris de constater à quel point les entreprises tolèrent les erreurs routinières dans le fonctionnement et la conception des contrôles de sécurité. Pendant ce temps, les équipes de direction continuent d'accepter un nombre faible, mais récurrent d'erreurs de contrôle, cédant par là même au fatalisme alors même que des solutions existent pour y remédier.

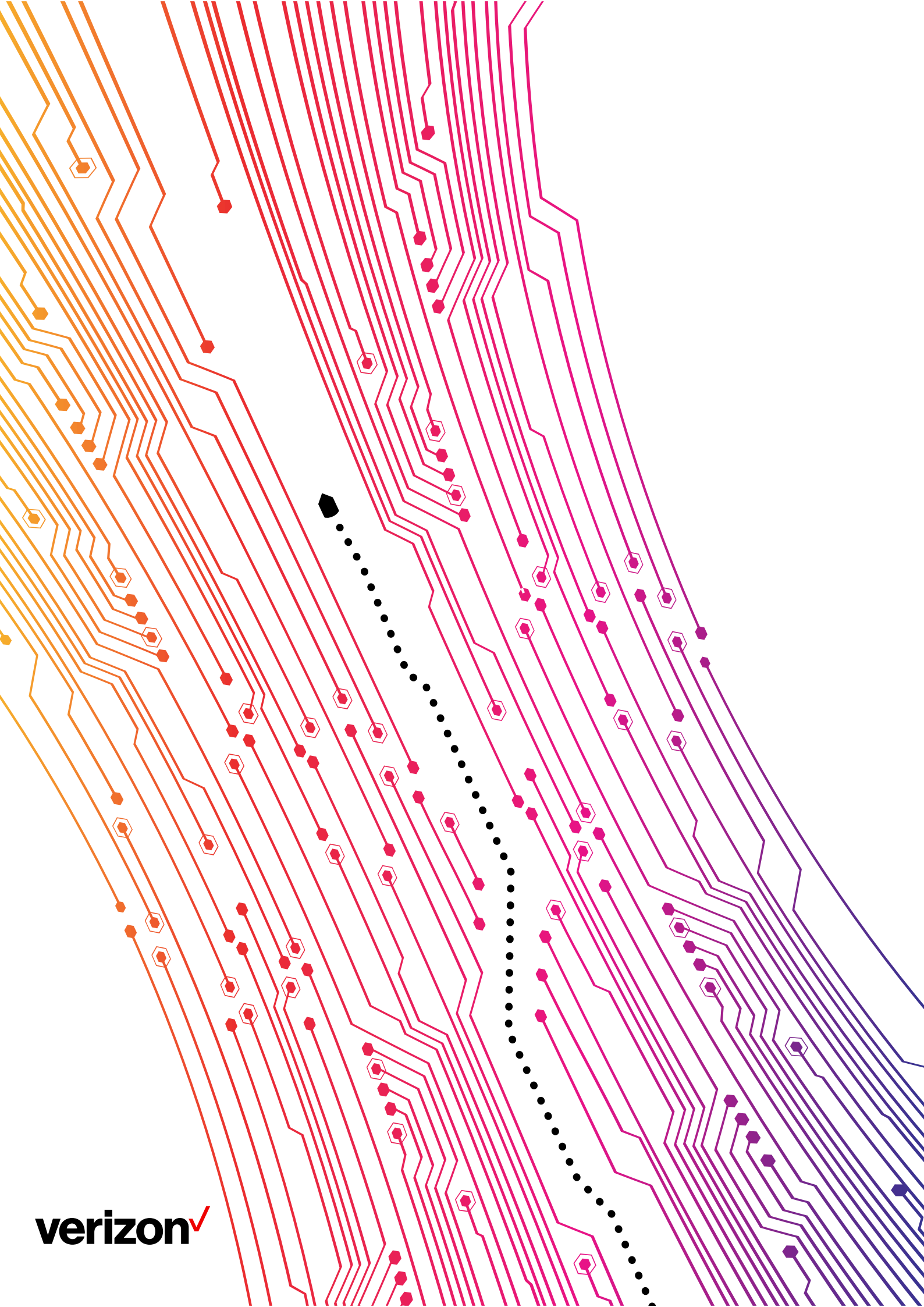
Pour plus d'informations autour du rapport PSR, rendez-vous sur : https://www.verizon.com/business/fr-fr/resources/reports/payment-security-report/

À propos de Verizon Cyber Security Consulting

Ce livre blanc a été rédigé par Verizon Cyber Security Consulting. Leader mondial de la sécurité pour l'industrie des cartes de paiement (PCI), Verizon Cyber Security Consulting compte dans ses rangs plus 600 consultants basés dans 30 pays et l'une des plus vastes équipes d'évaluateurs de sécurité PCI qualifiés – QSA – de la planète.

Verizon est le plus ancien fournisseur sur le marché des services PCI. Depuis 2002, l'entreprise offre à ses clients des conseils et des évaluations pour accroître la maturité de leurs programmes et garantir leur conformité aux standards SWIFT et PCI.

Son pôle Cyber Security Consulting les aide à identifier, détecter et contrer les cybermenaces afin de protéger leurs ressources et d'assurer la continuité de leurs activités, toujours dans le respect des standards et réglementations applicables.


verizon