

RAPPORT AUX RESPONSABLES DE LA GOUVERNANCE ET À LA DIRECTION

SOCIÉTÉ DE L'ASSURANCE AUTOMOBILE DU QUÉBEC
FONDS D'ASSURANCE AUTOMOBILE DU QUÉBEC
Audit des états financiers
de l'exercice clos le 31 décembre 2019



Sommaire du degré d'application des recommandations des exercices précédents

Fin de l'exercice					En cours d'application ¹		Total
	Recommandations appliquées (A)	Recommandations non appliquées (NA)	Sans objet ² (s. o.)	Recommandations caduques (C)	Progrès satisfaisants (PS)	Progrès insatisfaisants (PI)	
2017	-	-	1	-	-	-	1
Total	-	-	1	-	-	-	1

Recommandations des exercices précédents qui sont appliqués ou pour lesquels les progrès sont satisfaisants

Fin de l'exercice	Recommandations appliquées (A)	Progrès satisfaisants (PS)	Sous-total	Progrès insatisfaisants (PI)	Recommandations non appliquées (NA)	Total	Taux
Total							

-
1. Les travaux prévus pour l'appréciation des recommandations en cours d'application sont effectués avec un niveau d'assurance limité alors que les travaux sur les autres recommandations sont effectués avec un niveau d'assurance raisonnable.
 2. Le suivi de cette recommandation a été reporté (SR)

Catégorie et sujet		Adhésion de la direction		Degré d'application					
Catégorie	Gestion des technologies de l'information (GTI)	Oui	Non					En cours	
				A	NA	SR	C	PS	PI
Sujet	Gestion du développement et de la maintenance des systèmes	✓				✓			
Constatations		Recommandations		Commentaires de la direction pour les exercices antérieurs		Suivi			
Gestion des modifications aux systèmes Lors de nos travaux d'audit, nous avons constaté que les preuves des essais concernant les modifications de nature technique sur la plate-forme intermédiaire n'avaient pas toutes été conservées. Cette situation ne permet pas d'obtenir une assurance que les essais sont effectués adéquatement, en temps opportun et dans tous les cas. Des travaux d'audit supplémentaires ont dû être effectués afin de pallier cette déficience. Les résultats de ces travaux sont satisfaisants.		Nous recommandons à la SAAQ de : 1. Conserver les preuves de réalisation des essais concernant les modifications aux systèmes.		2017 La direction adhère aux recommandations formulées et mettra en œuvre le plan d'action proposé pour pallier les lacunes observées. 2018 La recommandation est appliquée et le plan d'action est mis en œuvre.		En 2019, il n'y a pas eu de modifications importantes de nature technique sur la plate-forme visée. Lors du prochain audit, s'il existe des modifications de cette nature, nous pourrions valider l'application de la recommandation.			

Catégorie et sujet		Adhésion de la direction	
Catégorie	Gestion des technologies de l'information (GTI)	Oui	Non
Sujet	Gestion des droits et des profils d'accès	✓	
Constatations	Recommandations	Commentaires de la direction	
Gestion des accès à CASA (SAP) Le 1^{er} janvier 2019, la Société a complété l'implantation de la Livraison 1 de son nouveau progiciel SAP, soit la solution opérationnelle – Gestion des ressources financières, matérielles & logistiques et de la relation client. Lors de la phase de développement, la Société a octroyé des accès à haut privilège pour permettre la réalisation de l'implantation. À la suite de la mise en production de SAP, nous avons constaté que l'accès à de très nombreux comptes à haut privilège n'a pas été retiré ou restreint selon le cas. Nous avons aussi noté ce qui suit : • Les privilèges à ces comptes donnent des pouvoirs substantiels, et leur utilisation ne fait pas l'objet d'un processus d'autorisation et de suivis systématiques; • Un nombre important de comptes possèdent des droits incompatibles. Ainsi, plusieurs développeurs ont accès à l'environnement de production. Ainsi, dans un rapport émis par la firme PWC en 2019, 12 recommandations ont été communiquées à la Société (5 avec une haute priorité, 6 avec une priorité moyenne et 1 avec une priorité basse).	La direction devrait prendre des mesures immédiates pour mettre en place les recommandations énoncées en lien avec les déficiences au niveau des accès à l'application SAP. Le plan d'action devrait, entre autres : 1. Instaurer un processus d'autorisation des accès à haut privilège. 2. Restreindre au minimum les accès à haut privilège et pour certains d'entre eux limiter leurs utilisations au strict minimum. 3. Assurer le suivi de la journalisation de l'utilisation des accès conservés. 4. Revoir les droits d'accès en fonction des rôles et responsabilités afin de corriger les problèmes de séparation des tâches incompatibles.	Effectivement, des mesures immédiates ont été prises : 1. Les principaux processus sont en place et opérationnalisés. Nous terminerons l'analyse des processus restants afin de les opérationnaliser au courant du 3^e trimestre. 2. Les analyses ont été effectuées, la majorité des corrections ont été réalisées (90 %) et nous terminerons la mise en place au courant du 3^e trimestre. (<i>adresser les recommandations du rapport PWC</i>) 3. Des actions sont déjà réalisées : • L'outil de suivi a été mis en fonction, • Le matériel de formation est produit, • Une analyse de l'utilisation est réalisée trimestriellement afin de valider l'utilisation normale des accès à haut privilège. La suite sera complétée dès le 4^e trimestre. 4. Les analyses ont été effectuées, la majorité des corrections ont été réalisées (80 %) et nous terminerons la mise en place au courant du 3^e trimestre. (<i>adresser les recommandations du rapport PWC</i>)	

Recommandations de l'exercice 2019

Constatations	Recommandations	Commentaires de la direction
L'importance des déficiences notées au niveau des accès à l'application SAP n'a pas permis d'utiliser une stratégie d'audit qui s'appuie sur les contrôles généraux des technologies de l'information (CGTI). En conséquence, la stratégie d'audit des données comptables provenant de SAP a dû être modifiée en ajoutant des procédures de corroboration afin de compenser les déficiences de contrôle. Ces déficiences de contrôle au niveau des accès à SAP ou d'autres enjeux au niveau des CGTI pourraient compromettre une stratégie d'audit qui s'appuie sur les CGTI de SAP pour l'exercice 2020 et les suivants et représenter un enjeu majeur pour l'exécution de l'audit des états financiers et entraîner des coûts additionnels importants. De plus, ces lacunes de contrôle augmentent le risque d'accès non autorisé pouvant compromettre l'exactitude et l'intégralité des données utilisées pour la production des états financiers de la Société et du Fonds d'assurance.		Le programme de transformation organisationnelle de la Société vise à mettre en place un nouveau modèle d'affaires et à moderniser ses principaux systèmes d'information, tant administratifs que de soutien à la mission datant de plus de 30 ans. L'un des principaux objectifs du programme est de permettre à l'organisation de faire évoluer ses solutions d'affaires, mais aussi de positionner avantageusement la Société dans l'actualisation de ses pratiques d'affaires ainsi que dans la mise en place d'un contexte favorable à leur évolution. La réalisation du programme est planifiée sur 2 livraisons réparties sur un horizon de 5 ans. Le défi était de livrer au jour 1 de la L1 l'ensemble des fonctionnalités, processus, formations et expertise des ressources pour opérer la solution. Or, les revues de processus, mandat de vérification, analyse d'écarts, constats et plans d'action suite à cette première mise en production nous ont permis d'identifier des pistes d'amélioration et des opportunités afin de bonifier nos contrôles sur les opérations et accroître notre maturité sur l'utilisation de notre solution d'affaires intégrée reposant sur les plus récentes technologies de l'information. Dans ce contexte, nous porterons une attention particulière aux CGTI.

Catégorie et sujet		Adhésion de la direction	
Catégorie	Gestion des technologies de l'information (GTI)	Oui	Non
Sujet	Gestion des droits et des profils d'accès	✓	
Constatations		Recommandations	
Gestion des retraits d'accès Lors de nos travaux d'audit, nous avons constaté les déficiences suivantes : • Suite à des départs de personnel, les accès n'ont pas été désactivés en temps opportun (4 cas testés sur un total de 18 tests); • Dans les cas où des utilisateurs réintègrent la Société après un départ de courte durée, celle-ci s'est montrée incapable de nous démontrer que le compte a bel et bien été désactivé promptement au moment de l'absence. Il y a donc une augmentation du risque d'accès non autorisé aux systèmes. Des travaux d'audit supplémentaires ont dû être effectués afin de pallier ces déficiences. Les résultats de ces travaux sont satisfaisants.		Commentaires de la direction 5 et 6 - Dès fin février 2020, un exercice d'épuration des accès informatique a été réalisé à partir de la banque de données du personnel de la direction des ressources humaines. Au 4 ^e trimestre, cet exercice sera refait. À la fin du 4 ^e trimestre, les ajustements au processus de gestion des arrivées et des départs des ressources internes et externes seront mis en place : • Révision des processus d'annulation des codes utilisateurs ayant quitté la Société; • Conservation des demandes et des preuves de désactivation; • Sensibilisation des gestionnaires vis-à-vis du suivi des mouvements de leurs personnels.	

Plan d'action

**Plan d'action de la direction pour l'application des recommandations
(recommandations de l'exercice et recommandations des exercices précédents en cours d'application)**

Recommandation n° 1 31 décembre 2017		Nous recommandons à la SAAQ de conserver les preuves de réalisation des essais concernant les modifications aux systèmes.		Commentaires
Constatations	Action ¹	Responsable	Échéance ²	
Les preuves des essais concernant les modifications de nature technique sur la plate-forme intermédiaire n'avaient pas toutes été conservées.	La recommandation est appliquée et le plan d'action est mis en œuvre.	VPTI	Déjà appliquée	

Plan d'action

Recommandations n ^{os} 1 à 4 31 décembre 2019		Nous recommandons à la Société d'instaurer un processus d'autorisation des accès à haut privilège, de restreindre au minimum les accès à haut privilège et pour certains d'entre eux limiter leurs utilisations au strict minimum, d'assurer le suivi de la journalisation de l'utilisation des accès conservés et de revoir les droits d'accès en fonction des rôles et responsabilités afin de corriger les problèmes de séparation des tâches incompatibles.		Commentaires
Constatations	Action ¹	Responsable	Échéance ²	
À la suite de la mise en production de SAP, nous avons constaté que l'accès à de très nombreux comptes à haut privilège n'a pas été retiré ou restreint selon le cas. (réf. recommandation #2)	Terminer de restreindre les accès à haut privilèges. Une validation par un pair est effectuée lors de la mise en place des corrections.	Centre de support CASA	T3	Pour chaque action, la Société procèdera à son évaluation afin d'assurer qu'elle permette d'appliquer la recommandation.
Les privilèges à ces comptes donnent des pouvoirs substantiels, et leur utilisation ne fait pas l'objet d'un processus d'autorisation et de suivis systématiques. (réf. recommandations #1, 3)	Autorisation - Terminer la mise en place du processus.	Centre de support CASA	T3	
	Suivis de la journalisation des accès - actions à venir : • Identifier les codes de transactions les plus sensibles • Mettre en place un processus permettant l'analyse rigoureuse des codes transactions identifiés au point précédent • Analyser rigoureusement les codes de transactions identifiés	DGSN Direction générale de la sécurité numérique	T4	
Un nombre important de comptes possèdent des droits incompatibles. Ainsi, plusieurs développeurs ont accès à l'environnement de production. (réf. recommandation #4)	Terminer la correction des droits incompatibles. Une validation par un pair est effectuée lors de la mise en place des corrections.	Centre de support CASA	T3	

Plan d'action

Recommandations n ^{os} 5 et 6 31 décembre 2019		Nous recommandons à la Société de désactiver promptement les accès suite au départ de personnel et de conserver les preuves de désactivation en tout temps lors de départs de courte durée.		Commentaires
Constatations	Action ¹	Responsable	Échéance ²	
Suite à des départs de personnel, les accès n'ont pas été désactivés en temps opportun. (réf. recommandation #5)	Épuration des accès informatiques à partir de la banque de données du personnel de la direction des ressources humaines.	DGSN Direction générale de la sécurité numérique	Février 2020 et T4	Pour chaque action, la Société procèdera à son évaluation afin d'assurer qu'elle permette d'appliquer la recommandation.
	Ajustements au processus de gestion des arrivées et des départs des ressources internes et externes : - Réviser les processus d'annulation des codes utilisateurs ayant quitté la Société - Sensibiliser les gestionnaires vis-à-vis du suivi des mouvements de leurs personnels		T4	
Dans les cas où des utilisateurs réintègrent la Société après un départ de courte durée, celle-ci s'est montrée incapable de nous démontrer que le compte a bel et bien été désactivé promptement au moment de l'absence. (réf. recommandation #6)	Ajustements au processus de gestion des arrivées et des départs des ressources internes et externes : Conserver des demandes et des preuves de désactivation	DGSN Direction générale de la sécurité numérique	T4	

1. Un des moyens pour s'assurer qu'une recommandation est appliquée est de prévoir notamment une action visant à évaluer si le problème est réglé.
2. L'échéance relative aux actions prévues peut varier mais, afin de favoriser une saine gestion, il importe de réaliser les actions le plus tôt possible.