Direction de la gouvernance, de l'architecture et de la réalisation des projets SI

Demande de dérogation – Validation des données converties réalisées par des ressources externes sans accompagnement d'un employé de la Société
Décembre 2021

CONTEXTE ET DEMANDE :

Voir référence courriel de la demande en annexe

Les travaux liés à la conversion des données dans le cadre de la livraison 2 du projet CASA sont importants et nécessitent plus d'efforts que prévus. Afin d'assurer que l'ensemble des données soit porté dans le nouvel environnement dans les temps requis et avec un niveau de qualité attendu, un plan d'action a été proposé par l'équipe du projet.

Jusqu'ici, selon leurs statuts (internes ou externes), il a été entendu au début du projet et est attendu que les ressources de l'équipe de conversion doivent suivre une procédure spécifique permettant de diminuer les risques d'accès aux données « nominalisées ». Différentes mesures et mécanismes de mitigation ont été mis en place dont plus spécifiquement, pour les ressources externes de l'alliance, l'obligation d'être accompagné par une ressource de la Société et de partager son écran lors de la réalisation de certains travaux.

Afin de gagner en vélocité et de pallier les enjeux du projet, il est demandé de déroger à cette façon de faire et permettre jusqu'à **13** nouvelles ressources de l'alliance de plus que les 27 personnes initialement identifiées en octobre 2021, de réaliser les activités de validation des données converties non anonymisée de façon autonome au même titre qu'une ressource interne. Sur ces 13 personnes, 3 d'entre elles ont déjà été identifiées, l'ajout de 10 ressources supplémentaires pourrait être effectué au cours de la période de dérogation selon les mêmes modalités.

La dérogation est demandée pour débuter **le 6 décembre 2021** et se terminer le **15 mai 2022 (EPV17).** Au besoin, une prolongation sera demandée.

Il est à noter que la présente analyse a également mis en lumière de nouveaux risques qui seront adressés dans ce document. De fait, considérant le contexte pandémique et le travail distant obligatoire, certaines mesures de mitigation initiales ont dû être adaptées afin de permettre la réalisation de ces activités tant pour les ressources internes que pour les ressources externes amenées à travailler dans la validation des données converties « nominalisées ».

ÉQUIPES IMPLIQUÉES :

Les équipes impliquées pour la réalisation des activités de validation des données sont les suivantes :

- Ressources du chapitre Conversion;
- Ressources provenant des autres équipes du projet CASA.

CONSIDÉRATIONS DE SÉCURITÉ :

Attentes initiales et recommandations de la gouvernance de la sécurité de l'information :

Adapté du courriel de Ghislain Marcotte, conseiller en sécurité de l'information, 29 mai 2017, annexe

- À titre de « Chef de projet CASA », Karl Malenfant est détenteur des données [redacted] CASA. De plus, depuis 2021, M. Malenfant porte également le rôle de gestionnaire délégué des données numériques gouvernementales. Par conséquent, il est légitimé d'autoriser la demande de dérogation.

- Considérant la nature hautement confidentielle et l'envergure de l'information contenue au dépôt de données [redacted]CASA, il est conseillé au détenteur, ou à son délégué, d'identifier les utilisateurs ayant accès à la « donnée nominalisée ». À cet effet, la tenue d'une liste à jour est recommandée. Cette liste sera fournie et maintenue par l'équipe du bureau de programme CASA.

- Concernant l'enquête de sécurité, le personnel externe tant de l'alliance que ceux embauchés par la Société doivent répondre aux exigences d'enquête de sécurité tel que stipulé au contrat établi avec le(s) fournisseur(s). Pour le personnel interne, tel qu'approuvé par le Comité de direction de la SAAQ, le niveau d'enquête suggérée est « habilitation sécuritaire ».

- Finalement, afin d'obtenir une piste administrative, il est important que la journalisation des accès soit activée et exploitable dans l'environnement [redacted]CASA.

ANALYSE DE RISQUE

Nom du risque	Exfiltration de données
Enjeux	Confidentialité et protection des renseignements personnels
Niveau du risque brut	Élevé

Description

Lors de la réalisation des essais de conversion et de validation des données converties, les employés autant internes qu'externes ont accès à des millions de dossiers non anonymisés (informations sensibles de contrats, de no carte de crédits, ou des renseignements personnels NAS, informations médicales, etc.). L'exfiltration massive de données est également possible.

Mesures de mitigation mise en place lors de la L1

- Production et mise à jour d'une liste des personnes désignées et limitées pour réaliser les essais et en limiter le nombre en fonction du nombre de postes de travail sécurisés disponibles;
- 12 postes de travail dédiés et sécurisés utilisés pour la réalisation des activités;
- Habilitation sécuritaire des ressources afin de vérifier les antécédents judicaires[1];
- Réalisation des essais dans la salle dédiée à la conversion qui est fermée et à accès restreint;
- Un bac de recyclage barré est disponible sur place pour récupérer les impressions nécessaires dans le cadre des essais;
- Une ressource interne supervise les étapes d'essais et de validation des données converties lorsque celles-ci sont réalisées par des ressources externes ;
- Restriction de l'accès aux postes et aux données via des comptes utilisateurs dédiés spécifiques (CUTV) activés et désactivés selon des modalités précises (voir annexe);
- Journalisation limitée permettant de surveiller l'accès aux postes et d'associer le compte utilisateur à celui-ci.

[1] Pour le personnel interne, cette habilitation a été bonifiée en 2021.

Niveau du risque résiduel L1	Faible

Mars 2021 : Début du télétravail

La livraison 1 est à ce stade terminée. Les mesures ont été maintenues pour la L2. Le contexte pandémique et le travail à distance obligatoire ont mené à certains assouplissements sur les moyens de mitigations initiaux pour l'ensemble des ressources impliquées qu'elles soient internes ou externes :

- Retrait de la réalisation des essais dans une salle dédiée à la conversion;
- Retrait de l'utilisation d'un bac de recyclage pour récupérer les impressions.

Dans ce contexte, toutes les ressources impliquées auront un accès direct à des données sensibles et des renseignements personnels de dossiers clients non anonymisés

Niveau du risque brut (Télétravail)	Moyen

Nouvelles mesures de mitigation

- Accès distant RDP sur les mêmes postes de travail dédiés et sécurisés (Ex. : aucun accès à Internet, impossibilité d'envoyer des courriels, etc.), spécifiquement configurés pour cette activité;
- Une ressource interne supervise via Teams (compagnonnage) les étapes de validation des données converties lorsque celles-ci sont réalisées par des ressources externes;
- Ces mesures minimisent les risques d'exfiltration massive de données et maintiennent la surveillance des données non anonymisées.

Niveau du risque résiduel (Télétravail)	Faible

Note : Pour la suite de l'analyse, une distinction a été établie entre la protection des renseignements personnels (exfiltration massive) et la confidentialité des données.

Octobre 2021 : Demande de dérogation	
Nom du risque	Exfiltration de données massive
Enjeux	Protection des renseignements personnels
Niveau du risque brut	Moyen

Description

- Permettre à 27 ressources externes de réaliser les activités de validation des données converties non anonymisée de façon autonome au même titre qu'une ressource interne;
- Retirer le contrôle actuel de compagnonnage des ressources externes par des ressources internes;
- Cette demande de dérogation met en lumière le risque que toutes les ressources internes ou externes ont accès aux données non anonymisées de manière autonome avec un accès distant sans surveillance visuelle.

Mesures de mitigation

- Toutes les ressources travaillent à partir du Canada;
- Toutes les ressources internes doivent faire l'objet d'une enquête d'habilitation sécuritaire et celles-ci doivent être approuvées par le comité aviseur de la SAAQ avant de pouvoir débuter les activités de validation;
- Toutes les ressources externes doivent faire l'objet d'une enquête d'habilitation sécuritaire tel que prévu au contrat et celles-ci doivent être approuvées par le Bureau de programme SAAQ avant de pouvoir débuter les activités de validation;
- Toutes les ressources autant internes qu'externes travaillent en accès distant sur des postes de travail dédiés et sécurisés (Ex. : aucun accès à Internet, impossibilité d'envoyer des courriels, etc.), spécifiquement configurés pour cette activité;
- Les accès aux données sont octroyés sur demande seulement;
- L'octroi est pour une période maximale de cinq (5) heures consécutives et les comptes sont désactivés automatiquement après ces cinq (5) heures;
- Ajout de postes supplémentaires sécurisés dans la salle dédiée aux essais et aux validations afin de permettre le travail en accès distant.

Niveau du risque résiduel	Faible

Octobre 2021 : Demande de dérogation	
Nom du risque	**Exfiltration de données**
Enjeux	**Confidentialité des renseignements personnels**
Niveau du risque brut	**Moyen**

Description

- Permettre à 27 ressources externes de réaliser les activités de validation des données converties non anonymisée de façon autonome au même titre qu'une ressource interne;
- Retirer le contrôle actuel de compagnonnage des ressources externes par des ressources internes;
- Cette demande de dérogation met en lumière le risque que toutes les ressources internes ou externes ont accès aux données non anonymisées de manière autonome avec un accès distant sans surveillance visuelle.

Mesures de mitigation

- Toutes les ressources travaillent à partir du Canada;
- Toutes les ressources internes doivent faire l'objet d'une enquête d'habilitation sécuritaire et celles-ci doivent être approuvées par le comité aviseur de la SAAQ avant de pouvoir débuter les activités de validation;
- Toutes les ressources externes doivent faire l'objet d'une enquête d'habilitation sécuritaire tel que prévu au contrat et celles-ci doivent être approuvées par le Bureau de programme SAAQ avant de pouvoir débuter les activités de validation;
- Toutes les ressources doivent signer à nouveau, le formulaire « Engagement de confidentialité avant le début des activités de validation » afin de confirmer leur intégrité morale envers la Société et leurs propres organisations selon le cas;
- Ce formulaire sera signé et déposé par les ressources avant le début des activités de validation;
- Toutes les ressources autant internes qu'externes travaillent en accès distant sur des postes de travail dédiés et sécurisés (Ex. : aucun accès à Internet, impossibilité d'envoyer des courriels, etc.), spécifiquement configurés pour cette activité;
- Ajout de postes supplémentaires sécurisés dans la salle dédiée aux essais et aux validations afin de permettre le travail en accès distant;
- Les accès aux données sont octroyés sur demande seulement;
- L'octroi est pour une période maximale de cinq (5) heures consécutives et les comptes sont désactivés automatiquement après ces cinq (5) heures;

Niveau du risque résiduel	**Moyen**

Nom du risque	Traçabilité des essais
Enjeux	Intégrité, Confidentialité
Niveau du risque brut	Élevé

Description

La journalisation est limitée à connaître sur quel poste un compte CUTV est connecté, elle ne permet pas de savoir avec certitude l'identité de l'individu ou dossier client à qui la donnée en cours de validation appartient.

- La journalisation de sécurité (SM20) des solutions SAP [redacted] et BW) ne permet pas de suivre précisément quelles données ont été consultées par l'utilisateur, mais permet d'identifier les transactions et programmes utilisés, et les tables consultées et exportées, le cas échéant;
- La journalisation dans l'outil de validation SAP Information Steward se limite aux informations de connexion des utilisateurs;
- La journalisation est suspendue pendant la conversion pour des raisons de performance.

Mesures de mitigation

- Journalisation active et exploitable de l'accès aux postes sécurisés permettant d'associer le compte et son accès;
- Minimiser les travaux de validation lors des sessions de conversions massives des données afin maintenir la journalisation active en tout temps;
- Production et mise à jour d'une liste des personnes désignées et limitées pour réaliser les essais et en limiter le nombre en fonction du nombre de postes de travail sécurisés disponibles;
- Toutes les ressources doivent signer à nouveau, le formulaire « Engagement de confidentialité avant le début des activités de validation » afin de confirmer leur intégrité morale envers la Société et leurs propres organisations selon le cas;
- Ce formulaire sera signé et déposé par les ressources avant le début des activités de validation;
- Un courriel de sensibilisation sur la sécurité des activités liées à la validation des données converties doit être transmis aux ressources visées.

Niveau du risque résiduel	Vert

Nom du risque	Facteur de l'opportunité
Enjeux	Confidentialité et vol de données
Niveau du risque brut	Faible

Description

Les ressources impliquées dans la conversion et la validation des données se sont portées volontaires amenant un risque supplémentaire d'atteinte à la confidentialité et aux vols de données.
Référence : Triangle de la fraude, annexe.

Mesures de mitigation

- Journalisation active et exploitable de l'accès aux postes sécurisés permettant d'associer le compte et son accès;
- Tout utilisateur (interne ou externe) accédant à des données confidentielles non anonymisées doit être en mesure de rapporter les objets qu'il a validés pour ainsi connaître l'ensemble des dossiers traités par chacun des valideurs.

Niveau du risque résiduel	Faible

RECOMMANDATION:

Conformément à la politique de sécurité de l'information et en fonction de la présente analyse, la direction de la gouvernance, de l'architecture et de la réalisation des projets SI recommande que le vice-président autorise :

- L'ajout de **3 nouvelles ressources** externes pour réaliser les activités de validation des données converties non anonymisée de façon autonome au même titre qu'une ressource interne ;
- Le retrait du contrôle actuel de compagnonnage des ressources externes par des ressources internes;
- Toutes les ressources internes ou externes à avoir accès aux données non anonymisées de manière autonome avec un accès distant.

Préparée par : Rémy Lapointe, Louis-David Sirois, Véronique Girard et Steve Bolduc, Direction de la gouvernance, de l'architecture et de la réalisation des projets SI

Validée par : Damien Bilodeau, directeur général de la sécurité de l'information

Signature [redacted]

Caroline Foldes-Busque, Leader Livraison 2, Carrefour des services d'affaires (CASA)

*Signature*_____

Approuvée par : Karl Malenfant, vice-président aux ressources humaines, matérielles et aux services numériques

*Signature*_____