Health Canada Santé Canada

Rapport de vérification final

Vérification de l'intégrité des données

Système d'information sur la santé et de traitement des demandes de paiement (SISTDP)

octobre 2008

Table des matières

Résumé

Le Système d'information sur la santé et de traitement des demandes de paiement (SISTDP) sert à traiter les demandes concernant le Programme des services de santé non assurés (PSSNA). Il s'agit de l'un des nombreux systèmes qui alimentent en données le système SAP, soit le système financier du Ministère. Depuis 1990, Santé Canada fait appel à un entrepreneur pour assurer la prestation des services d'information sur la santé et de traitement des demandes de paiement relatives aux composantes du PSSNA liées aux médicaments, fournitures et équipements médicaux, ainsi qu'aux soins dentaires. À son tour, l'entrepreneur a confié en sous-traitance à une tierce partie le traitement d'une grande partie de ces demandes. En 2006-2007, la somme de ces demandes s'élevait à environ 545 millions de dollars.

Les objectifs de la vérification étaient les suivants :

déterminer l'intégralité et l'exactitude des données du SISTDP qui sont téléchargées vers le système financier de Santé Canada;

fournir une évaluation générale de l'environnement de contrôle interne lié au Système d'information sur la santé et de traitement des demandes de paiement.

Le Bureau de la vérification et de la responsabilisation a mené la vérification conformément à la Politique sur la vérification interne du gouvernement du Canada.

Au cours de cette vérification, nous n'avons relevé aucun problème majeur en ce qui a trait à l'exactitude et à l'intégralité des données. Toutefois, nous avons noté que la conception du SISTDP permettait aux employés affectés au PSSNA – lesquels sont autorisés à entrer des données et à les mettre à jour – d'entrer des honoraires pour services dentaires qui pouvaient dépasser le montant maximal permis. Si cette situation se produisait, elle pourrait entraîner le versement d'un trop-payé à un dentiste.

En général, l'environnement de contrôle du SISTDP est satisfaisant. Cependant, les activités des utilisateurs finaux ne sont surveillées ni au chapitre de l'application, ni au chapitre des bases de données. Nous avons également constaté que les documents relatifs à l'octroi de privilèges d'accès au SISTDP au personnel affecté au PSSNA étaient incomplets. Ces constatations indiquent un risque d'accès non autorisé à l'application ou à la base de données du SISTDP.

Introduction

Contexte

Le Programme des services de santé non assurés (PSSNA) de la Direction générale de la santé des Premières Nations et des Inuits (DGSPNI) est le plus important programme de Santé Canada, représentant environ 29 % du budget total du Ministère. Il finance – à l'intention de quelque 780 000 membres inscrits des Premières Nations et Inuits reconnus – un éventail de produits et de services médicaux nécessaires, lesquels ne sont pas couverts par les régimes d'assurances privés, les programmes sociaux et d'assurance-maladie territoriaux ou provinciaux, ou les autres programmes financés par l'État.

Depuis 1990, Santé Canada donne en sous-traitance la prestation des services d'information sur la santé et de traitement des demandes de paiement afin qu'un entrepreneur gère les demandes relatives aux composantes du PSSNA liées aux médicaments, fournitures et équipements médicaux, ainsi qu'aux soins dentaires. À son tour, l'entrepreneur confie en sous-traitance à une tierce partie le fonctionnement du Système d'information sur la santé et de traitement des demandes de paiement (SISTDP), soit le système qui traite des demandes de paiement relatives à ces composantes. Le SISTDP est l'un des nombreux systèmes qui alimentent le système financier du Ministère (système SAP) en données. Au cours de l'exercice de 2006-2007, le SISTDP a traité des demandes dont le montant totalise environ 545 millions de dollars.

En ce qui concerne le SISTDP, les principales responsabilités incombant au sous-traitant comprennent, entre autres, les suivantes :

assurer le traitement des demandes de paiement relatives aux médicaments, fournitures et équipements médicaux, ainsi qu'aux soins dentaires;

offrir le SISTDP, en assurer l'exploitation, y apporter les modifications nécessaires et maintenir sa base de données.

Le SISTDP comprend tous les services et les systèmes permettant d'effectuer le traitement des demandes de paiement liées au PSSNA; de traiter et de régler des demandes provenant des fournisseurs de services; et d'assurer le respect des politiques régissant le PSSNA – y compris celles qui concernent la vérification, l'établissement de rapports et les pratiques de contrôle financier.

Au moment de la vérification, environ 99 % des demandes de paiement liées aux produits pharmaceutiques et 44 % de celles liées aux frais dentaires remplies par les fournisseurs de services étaient transmises par voie électronique au moyen d'un réseau d'échange de données informatisées (EDI). Toutes les demandes de paiement de fournitures et d'équipements médicaux ont été présentées manuellement. L'entrepreneur traite toutes les demandes qui requièrent l'entrée manuelle de données.

À l'Annexe A, nous présentons un aperçu de l'architecture du SISTDP, qui soutient le traitement informatisé des demandes de paiement.

La vérification a été entreprise par le Bureau de la vérification et de la responsabilisation conformément au plan de vérification fondée sur les risques, adopté par Santé Canada, lequel a été approuvé par le Comité ministériel de vérification et d'évaluation le 4 octobre 2006. La vérification a été menée en conformité avec la Politique sur la vérification interne du gouvernement du Canada.

Objectifs

Les deux objectifs de la vérification consistaient à :

- déterminer l'intégralité et l'exactitude des données du SISTDP qui sont téléchargées vers le système financier de Santé Canada;
- fournir une évaluation générale de l'environnement de contrôle interne lié au Système d'information sur la santé et de traitement des demandes de paiement.

Voici les deux secteurs d'intérêt faisant l'objet de la vérification :

- **L'intégralité et l'exactitude des données relatives aux demandes**

  Ce secteur d'intérêt englobait les éléments suivants :

  - les mesures de contrôle visant à s'assurer que les transactions sont traitées de façon exacte et complète;
  - la répartition des tâches liées au traitement des transactions;
  - l'exactitude et l'intégralité des données relatives aux demandes qui sont téléchargées vers le système SAP;
  - le processus permettant de repérer et de corriger à temps les transactions qui ont été traitées de façon erronée (traitement des erreurs)

- **L'environnement général de contrôle visant à limiter l'accès au système**

  Ce secteur d'intérêt englobait les éléments suivants :

  - l'examen par la direction des comptes d'utilisateur;
  - l'accès au SISTDP par les employés affectés au PSSNA;
  - l'accès au système par les administrateurs de la base de données (ABD);
  - la gestion de problèmes;
  - les procédures de sauvegarde et de restauration.

Étendue et démarche

La vérification a porté sur l'exactitude et l'intégralité des données du SISTDP en ce qui a trait au traitement des demandes relatives aux médicaments, fournitures et équipements médicaux, ainsi qu'aux soins dentaires. Les travaux ont été effectués au bureau des opérations du PSSNA dans la région de la capitale nationale, à First Canadian Health à Toronto et au bureau des opérations du sous-traitant à Mississauga.

Nous n'avons pas examiné la validité des demandes traitées au moyen du réseau d'échange de données informatisées (EDI). Cela aurait supposé l'examen du réseau, ce qui dépasse la portée de la vérification.

La vérification a été menée à l'aide des critères inspirés du modèle de gouvernance des TI de l'Association des professionnels de la vérification et du contrôle des systèmes d'information (APVCSI) – Objectifs de contrôle de l'information et des technologies connexes (COBIT = Control Objectives for Information and Related Technology); des manuels ministériels sur les procédures administratives; et de la politique sur la sécurité de la TI de Santé Canada.

Les entrevues ont été menées auprès d'experts fonctionnels affectés au PSSNA, de l'entrepreneur et du sous-traitant. Nous avons examiné des documents concernant le SISTDP. Parmi ces documents, mentionnons des documents sur la conception détaillée, des manuels de procédures administratives, des manuels de formation et d'autres manuels techniques. Nous avons également effectué des tests sur les contrôles informatiques généraux et sur ceux liés aux applications spécifiques, et nous avons procédé à des tests détaillés sur les bases de données portant sur les services pharmaceutiques, les fournitures et les équipements médicaux, ainsi que les soins dentaires, pour les mois d'avril, de juillet et d'octobre 2006, et d'avril 2007. En outre, nous avons vérifié l'exactitude de l'entrée des données, des contrôles d'accès, du traitement et de la journalisation des exceptions et des autorisations, et des procédures de sauvegarde et de restauration.

Constatations, recommandations et réponses de la direction

Intégralité et exactitude des données

Traitement des données d'entrée, et les données de sortie

Selon les pratiques exemplaires, les données à traiter doivent faire l'objet de divers contrôles afin que l'on puisse vérifier leur exactitude, leur intégralité et leur validité. Il devrait y avoir des procédures permettant de corriger toute erreur détectée le plus tôt possible au cours du processus. On doit procéder à un examen régulier des données de sortie afin de s'assurer qu'elles reflètent les données entrées à l'origine.

Nous avons examiné un échantillon de 26 demandes ayant été entrées dans le SISTDP afin d'en évaluer la validité, l'exactitude et l'intégralité. Nous avons également examiné les documents relatifs aux procédures afin de nous assurer qu'ils comprenaient des contrôles clés, comme la répartition des tâches et des contrôles d'entrée de données (contrôles permettant de s'assurer que seules les données valides sont traitées). L'équipe de vérification a également évalué la mesure dans laquelle les tâches étaient réparties et si le processus d'entrée de données était lié aux demandes de prestations.

Nous n'avons découvert aucun écart entre les documents sources examinés et les bases de données portant sur les services pharmaceutiques, les fournitures et les équipements médicaux, et les soins dentaires. Nous avons vérifié le processus de rapprochement pour les mois d'avril, de juillet et d'octobre 2006 et d'avril 2007 afin de déterminer l'exactitude et l'intégralité des données téléchargées vers le système financier de Santé Canada. Aucun écart majeur n'a été constaté.

Nous avons noté que le SISTDP possède de nombreuses caractéristiques visant à s'assurer que les données relatives aux demandes sont traitées de façon exhaustive et précise. Toutefois, les tests détaillés que nous avons effectués à l'égard des données relatives aux demandes de remboursement des frais dentaires nous a permis de relever 150 transactions – effectuées en septembre et décembre 2006 – où le champ « honoraires professionnels approuvés » avait été modifié par un employé affecté au PSSNA afin qu'il corresponde aux honoraires professionnels applicables au moment du paiement. Voici la justification donnée par les responsables du PSSNA pour cette dérogation par rapport au montant maximal fixé pour les honoraires professionnels :

i. composer avec des circonstances comme des délais inattendus dans la mise à jour des honoraires pour services professionnels; ou

ii. tenir compte des cas où le dentiste, se rendant compte que la procédure dentaire se révèle plus complexe que ce qu'il avait estimé, soumet une demande qui est supérieure au montant maximum permis pour soins dentaires.

Le fait que le système permet aux employés affectés au PSSNA de passer outre le champ « honoraires professionnels approuvés » et d'entrer un montant différent expose le Ministère au risque que des honoraires inappropriés pourraient être entrés dans le système et payés. Cette situation doit donc être étroitement surveillée. Au moment de l'exécution de notre vérification, les employés affectés au PSSNA ne surveillaient pas ces cas de dérogation.

Recommandation 1

Il est recommandé que le sous-ministre adjoint, Direction générale de la santé des Premières Nations et des Inuits, veille à ce qu'un agent supérieur affecté au PSSNA examine et approuve toutes les transactions où les honoraires professionnels approuvés excèdent le montant maximum d'honoraires pour soins dentaires permis par le SISTDP.

Réponse de la direction

La fonctionnalité qui permet aux agents de fixer les honoraires à payer au-delà du montant normalement permis est liée à une exigence opérationnelle. La Direction des services de santé non assurés convient que les contrôles s'appliquant à cette fonctionnalité s'avèrent insuffisants et mettra en œuvre des mesures permettant une supervision appropriée dans les cas où les agents de Santé Canada augmentent les honoraires professionnels approuvés afin de régler les situations où les honoraires permis dans le cadre du PSSNA ne suffisent pas à défrayer les professionnels de la santé des coûts réels engagés en raison des besoins particuliers du client.

Environnement de contrôle général

Nous nous attendions à ce que la direction ait établi un processus permettant l'examen, la confirmation et la surveillance des droits d'accès de tous les utilisateurs et à ce qu'elle examine périodiquement les accès au système et les transactions qui ont eu lieu. Selon les pratiques exemplaires, on doit également gérer les mots de passe de façon appropriée afin de contrôler l'accès au système.

Nous avons constaté que l'environnement de contrôle relatif au SISTDP est satisfaisant en général. Cependant, nous avons deux préoccupations. Tout d'abord, nous signalons qu'il n'y a aucune surveillance des activités d'utilisation du SISTDP, y compris les activités relatives aux bases de données. Nous avons également noté qu'on ne consignait pas de façon exhaustive l'octroi de privilèges d'accès au SISTDP aux employés. Cette démarche et les documents qui en découlent sont d'une importance capitale pour garantir que seul le personnel autorisé peut accéder aux données du SISTDP.

Examen par la direction des activités des utilisateurs

Nous n'avons trouvé aucun document probant attestant que la direction fait un suivi régulier des membres du personnel affectés au PSSNA qui ont accédé à l'application du SISTDP. La direction ne surveille pas les activités d'utilisation du SISTDP, ni l'accès à la base de données par les administrateurs de la base de données (ABD) travaillant aux installations du sous-traitant. Cette situation nous préoccupe parce que les ABD, contrairement à d'autres utilisateurs, disposent d'un accès illimité à la base de données, y compris la capacité d'y apporter des changements.

Nous notons que des rapports rédigés aux fins de suivi et de surveillance pourraient être mis à la disposition de la direction. Le système a la capacité de générer des journaux qui indiquent les transactions effectuées et le nom des personnes ayant accédé au système et qui, ainsi, peuvent constituer une piste de vérification. Toutefois, au moment de la vérification, le sous-traitant n'avait pas activé la fonction relative à la piste de vérification parce qu'elle consomme une grande quantité de ressources informatiques et qu'elle nuit au rendement du système.

Parce que cette fonction n'a pas été activée, aucune surveillance n'a été exercée sur les activités liées au SISTDP. Par conséquent, la direction n'avait aucun moyen de savoir si des activités irrégulières ou des accès potentiellement inappropriés à la base de données avaient eu lieu.

Le fait qu'on n'utilise pas l'information disponible pour examiner périodiquement les activités liées au système de tous les utilisateurs, y compris les ABD, on expose le Ministère au risque que quelqu'un pourrait accéder aux données du SISTDP ou y apporter des modifications non autorisées (compromettant ainsi leur exactitude et leur intégralité) et ce, sans que le ministère ne soit en mesure de déterminer qui est responsable de ces actes.

Nous avons également remarqué que les administrateurs de la base de données, travaillant aux installations du sous-traitant, pouvaient faire un nombre illimité de tentatives infructueuses pour entrer dans le système sans jamais en être bloqués. Il y a donc un risque qu'une personne de ce groupe puisse, par un procédé d'essais et erreurs, trouver un mot de passe qui lui donnerait accès au système sans l'autorisation appropriée.

Recommandation 2

Il est recommandé que le Sous-ministre adjoint de la Direction générale de la santé des Premières Nations et des Inuits veille à ce que les activités de tous les utilisateurs qui ont accès au Système d'information sur la santé et de traitement des demandes de paiement, y compris à la base de données, fassent l'objet d'une surveillance périodique. Cette surveillance devrait porter sur les activités liées à l'application qu'effectue le personnel affecté au PSSNA et sur celles liées à la base de données que mènent les administrateurs de la base de données travaillant pour le sous-traitant.

Réponse de la direction

La Direction des services de santé non assurés est d'accord avec la recommandation. Ce problème a déjà été cerné par les responsables du Programme et on a intégré de nouvelles exigences dans l'énoncé de travail relatif au nouveau SISTDP qui est en cours de mise au point.

Administration des privilèges d'accès

Selon les pratiques exemplaires et la politique sur la sécurité du Ministère, les droits d'accès de tout utilisateur devraient être documentés. Nous nous attendions à trouver un registre à jour de tous les employés, affectés au PSSNA, qui ont l'autorisation d'accéder au système, et à ce que ce registre indique les opérations que ces employés ont le droit d'effectuer dans le système et le nom de la personne ou du service qui a donné cette autorisation. Cette information devrait être inscrite sur des formulaires de demande de sécurité, qui devraient être conservés pendant au moins trois ans, comme l'exige la politique du gouvernement sur les fonds d'information.

Nous avons constaté qu'un certain nombre de formulaires de demande de sécurité de notre échantillon étaient incomplets. Par exemple, certains n'indiquaient pas le nom de la personne qui avait demandé l'autorisation afin que certains employés soient autorisés à avoir accès au système, ou encore celui de la personne qui leur avait finalement accordé cette autorisation. D'autres formulaires de demande de sécurité avaient été jetés au rebut par le sous-traitant après seulement un an.

Recommandation 3

Il est recommandé que le Sous-ministre adjoint de la Direction générale de santé des Premières Nations et des Inuits veille à ce que :

(a) tous les formulaires de sécurité soient conservés pendant au moins trois ans (c.-à-d. conformément à la Politique sur la gestion de l'information);
(b) tous les formulaires de demande de sécurité ne soient approuvés que par le personnel autorisé;
(c) tous les formulaires de demande de sécurité soient signés par les membres désignés de la direction.

Réponse de la direction

La Direction des services de santé non assurés est d'accord avec cette recommandation et a déjà pris des mesures visant à résoudre ce problème. Un rapprochement complet, c.-à-d. une comparaison des listes d'utilisateurs à Santé Canada, a été effectué à la suite d'une évaluation des facteurs relatifs à la vie privée effectuée par les responsables du Programme en juin 2006. Ce rapprochement a permis de garantir que seuls les utilisateurs autorisés ont accès au SISTDP actuel.

Gestion des problèmes

Nous nous attendions à ce que la direction du PSSNA ait mis en œuvre un système permettant de s'assurer que tous les incidents, problèmes et erreurs opérationnels sont rapidement relevés, analysés et résolus en temps opportun.

Les problèmes relevés quant au SISTDP sont classés dans l'une ou l'autre de quatre catégories – « problèmes critiques », « problèmes d'importance élevée », « problèmes d'importance moyenne » ou « problèmes de faible importance » –, et on leur accorde un degré de priorité correspondant. Aux fins de notre vérification, nous nous sommes concentrés sur les « problèmes critiques » inscrits dans quatre registres de problèmes conservés par l'entrepreneur et le sous-traitant afin de fournir une assurance que ces problèmes étaient réglés sans retard déraisonnable. Par « problème critique », on entend « *un problème lié au système qui entrave la prestation de services et pour lequel il n'existe aucune solution de rechange raisonnable, que celle-ci soit informatisée ou manuelle (la solution de rechange nécessiterait beaucoup de temps, exigerait beaucoup d'interactions humaines ou serait propice à des erreurs humaines répétées); qui constitue un risque pour la santé et la sécurité du client; qui fait augmenter les coûts liés au programme; qui compromet l'intégrité des données du client, des données financières ou des données du fournisseur; qui dérange cinq utilisateurs ou plus ou une région/un bureau en entier; ou qui compromet la sécurité du système* [traduction] ».

En analysant les registres des problèmes, nous avons relevé au total 176 problèmes critiques. De ce nombre, 24 % avaient été résolus en 48 heures ou moins. Nous avons découvert qu'il a fallu plus de 2 mois pour résoudre 38 % des problèmes critiques.

Bien qu'un programme d'incitation au rendement ait été mis en œuvre durant l'année de contrat 2007, nous avons noté qu'il n'existe aucune entente officielle entre l'entrepreneur et son sous-traitant dans lequel on établit des normes raisonnables relatives au délai pour résoudre les problèmes ***critiques*** (voir la définition ci-dessus). Dans le cadre dudit programme, on incite les gens à résoudre les problèmes critiques dans un délai de un à 12 mois.

Le fait de mettre beaucoup de temps à résoudre des problèmes critiques constitue une préoccupation, étant donné le risque d'entrave à la prestation de services, les risques pour la santé et la sécurité du client, les risques d'augmentation des coûts liés au programme, ou encore le risque que soit compromise l'intégrité des données du client, des données financières ou des données de l'entrepreneur.

Recommandation 4

Il est recommandé que le Sous-ministre adjoint de la Direction générale de santé des Premières Nations et des Inuits veille à ce que les normes convenues avec l'entrepreneur/le sous-traitant à l'égard de la résolution de problèmes critiques stipulent un délai plus court.

Réponse de la direction

La Direction des services de santé non assurés convient que la résolution rapide des problèmes liés au système de traitement des demandes mérite une attention continuelle. Grâce à des négociations, dans le cadre du PSSNA, des progrès importants ont été réalisés au chapitre de la réduction de la liste des problèmes et de l'amélioration de la gestion et de la résolution des problèmes conformément aux conditions du contrat. En vertu du contrat établi en 1997, la Direction des services de santé non assurés n'est pas bien placée pour inciter l'entrepreneur à l'action et a donc décidé d'imposer de nouvelles exigences au nouvel entrepreneur afin qu'il mette en œuvre des normes relatives à la résolution de problèmes. L'entrepreneur sera également tenu, conformément aux conditions du nouveau contrat, de veiller à ce que ces exigences s'appliquent à tout sous-traitant. Dans le but d'accomplir de vrais progrès à court terme, la Direction du PSSNA déploie plus d'efforts à l'étape de la mise à l'essai du système pour réduire les possibilités d'erreurs, et elle collabore continuellement avec l'entrepreneur/ l'entrepreneur principal pour déterminer des trucs et solutions de rechange efficaces et rapides, et pour classer les travaux par ordre de priorité en fonction du risque. Aucun des problèmes sur lesquels on travaille actuellement ne crée de risques pour la santé ou n'expose le Ministère à des risques financiers, et le registre des problèmes fait l'objet d'un processus d'examen conjoint régulier visant l'établissement de l'ordre de priorité des problèmes à régler en fonction des risques. On a pris des mesures pour améliorer le processus de gestion des incidents et les normes qui s'y rattachent, conformément aux conditions du nouveau contrat concernant le SISTDP, et pour s'assurer que ces exigences s'appliqueront à tout sous-traitant.

Sauvegarde et restauration

Il devrait y avoir des procédures documentées servant à définir et à mettre en œuvre les mesures de secours informatique et de rétablissement des données du système dans le cadre d'un plan de continuité des opérations et de reprise après sinistre. Il devrait également y avoir des mesures de sauvegarde adéquates permettant de protéger les données. Nous avons vérifié la conformité avec les procédures et les pratiques exemplaires requises pour que le système et ses données fassent l'objet de sauvegardes adéquates et, le cas échéant, pour qu'ils soient restaurés. Nous avons constaté que le sous-traitant respectait les procédures exigées relativement à la sauvegarde, au rétablissement et à la protection du système et de ses données.

Annexe A : Secteurs d'intérêt et critère de vérification

SECTEURS D'INTÉRÊT	CRITÈRES DE VÉRIFICATION
A. L'intégralité et l'exactitude des données relatives aux demandes	
Les contrôles permettant d'assurer que les transactions sont traitées de façon exacte et complète	• Les procédures permettent d'obtenir une assurance à l'effet que tous les documents sources autorisés sont complets et exacts, bien pris en compte et transmis rapidement pour être traités. • Les données sur les transactions entrées dans le système pour traitement (données générées par des gens, un système ou un interface) devraient faire l'objet de divers contrôles afin que l'on puisse obtenir une assurance sur leur exactitude, leur exhaustivité et leur validité.
La répartition des tâches liées au traitement des transactions	• Le personnel autorisé, agissant dans son champ de compétence, prépare les documents sources, et il existe une répartition adéquate des tâches au sujet de la création et de l'approbation des documents sources.
L'exactitude et l'intégralité des données relatives aux demandes qui sont téléchargées vers le système SAP	• Les extrants sont régulièrement comparés aux totaux de contrôle pertinents. Des pistes de vérification facilitent le retracement du traitement des transactions et le rapprochement des données dont le traitement a été interrompu.
Le processus permettant de repérer et de corriger rapidement les transactions qui ont été traitées de façon erronée (traitement des erreurs)	• Il existe des procédures pour la correction et le retraitement des données qui ont été traitées de façon erronée, et ces procédures sont respectées. • Des procédures pour composer avec les erreurs commises pendant la création des données devraient permettre l'obtention d'une assurance raisonnable que toute erreur ou irrégularité est détectée, déclarée et corrigée.
B. L'environnement général de contrôle visant à limiter l'accès au système	
L'examen par la direction des comptes utilisateurs	• La direction devrait avoir un processus de contrôle en place pour que les droits d'accès fassent périodiquement l'objet d'examen et de confirmation.
L'accès au SISTDP par les employés affectés au PSSNA est contrôlé et surveillé	• Les droits d'accès aux systèmes et aux données devraient correspondre aux besoins fonctionnels et aux exigences du poste, lesquels besoins et exigences ont été définis et documentés. Les droits d'accès sont demandés par les dirigeants de l'utilisateur, approuvés par le propriétaire du système et mis en œuvre par la personne responsable de la sécurité.
L'accès au système par les administrateurs de la base de données (ABD) est contrôlé et fait périodiquement l'objet d'un examen.	• Veiller à ce que la direction du compte utilisateur s'occupe de la demande, de l'établissement, de l'octroi, de la suspension, de la modification et de la fermeture de tout compte utilisateur et des privilèges connexes. Il doit y avoir une procédure d'approbation précisant le propriétaire des données ou du système qui accorde les privilèges d'accès. Cette procédure devrait s'appliquer à tous les utilisateurs qu'ils soient internes ou externes, y compris les administrateurs (utilisateurs privilégiés).
Il y a en place un système de gestion des problèmes et ceux-ci sont réglés rapidement.	L'organisation devrait instaurer des procédures pour composer avec les erreurs commises durant le traitement des données, soit des procédures qui permettent le repérage des transactions erronées avant qu'elles ne soient traitées et sans causer une interruption excessive des autres transactions valides.
Il y a en place des procédures de sauvegarde et de restauration.	• Définir et instaurer des procédures pour assurer la sauvegarde et la restauration des systèmes, des données et de la documentation conformément aux exigences fonctionnelles et au plan de continuité. Vérifier la conformité par rapport aux procédures de sauvegarde, et vérifier non seulement la capacité de procéder à une restauration complète et réussie, mais aussi le temps requis pour ce faire. Effectuer des tests sur les moyens de sauvegarde et le processus de restauration.

Les critères de vérification ont été résumés aux fins de présentation.

Annexe B : Architecture de Système