Vérification interne

Rapport du vérificateur

# Vérification du Système informatisé de gestion des subventions et bourses du CRSNG

# TABLE DES MATIÈRES

# 1. RÉSUMÉ

Le Conseil de recherches en sciences naturelles et en génie (CRSNG) a exigé une vérification de son système informatisé de gestion des subventions et bourses (SIGSB).

Le SIGSB sert à gérer et à suivre le cycle de vie de l'octroi de subventions du CRSNG, à enregistrer les demandes de subvention initiales, à effectuer la sélection par les pairs, à enregistrer l'approbation finale des subventions et à gérer le financement des subventions. Le SIGSB permet aussi au CRSNG de suivre l'état du financement. De plus, le système possède une interface automatisée avec le système financier d'achat et de gestion des actifs immobilisés (SFAGAI).

Les objectifs de la vérification étaient les suivants :

1. s'assurer que le SIGSB respecte les règles administratives améliorées nécessaires afin :
    - de garantir l'intégrité des données,
    - de gérer et desuivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG,
    - d'accepter et d'enregistrer la demande initiale,
    - d'observer la sélection par les pairs,
    - de gérer les subventions post-octrois,
    - de communiquer des données;
2. s'assurer que le SIGSB comprend les contrôles nécessaires pour le suivi du financement et des paiements;
3. s'assurer que le système possède les contrôles nécessaires pour toute information financière du SIGSB transmise au SFAGAI;
4. établir la pertinence du cadre de contrôle de gestion (sujet abordé dans la conclusion générale);
5. établir l'efficacité du SIGSB en ce qui a trait à sa convivialité, l'ampleur de sa portée, etc.

La délimitation de la vérification, telle que précisée par le CRSNG (vérification interne), comprend le SIGSB ainsi que l'interface avec le SFAGAI.

La vérification a été effectuée selon la méthodologie de vérification internationale pour l'évaluation de contrôles informatiques de Deloitte & Touche LLP; il s'agit d'une démarche exhaustive axée sur le risque et mise au point en totalité par les experts en la matière de Deloitte & Touche. Cette démarche est complétée par les meilleures pratiques utilisées par des spécialistes à l'échelle internationale. En particulier, la méthodologie de propriété comprend deux programmes de vérification pour l'évaluation : *1) contrôles informatiques généraux* et *2) contrôles des processus opérationnels*. Ainsi, les contrôles du SIGSB ont été documentés et évalués en les comparant à un cadre de contrôle rigoureux et les recommandations à l'intention du CRSNG visaient à faciliter la mise en oeuvre des mécanismes de contrôle nécessaires.

En ce qui concerne l'objectif de la vérification portant sur la convivialité et l'ampleur de la portée, quatre groupes de consultation ont été formés pour recueillir les commentaires des intervenants sur le niveau de satisfaction pour divers éléments du système. Ces consultations ont été menées avec l'aide d'une technologie de vote anonyme.

La vérification interne a été effectuée selon la politique du Conseil du Trésor sur la vérification interne et les normes de l'institut des vérificateurs internes.

Nous avons conclu que les contrôles des processus opérationnels sont convenables à l'appui des objectifs de

la vérification, toutefois les contrôles informatiques généraux dans certains secteurs ne semblent pas appuyer le traitement du SIGSB de façon efficace. De plus, il existe des risques liés à l'accès au SIGSB et à la séparation des tâches. Malgré la présence de certaines forces, nous avons conclu que l'ensemble du cadre de contrôle n'est pas adapté aux risques identifiés.

De façon globale, nous croyons que les contrôles internes dans les secteurs d'application et de sécurité logique et d'entretien et de développement de système méritent une amélioration considérable.

En ce qui a trait à la convivialité et l'ampleur de la portée du SIGSB, nous avons conclu que, même si les utilisateurs du SIGSB sont généralement satisfaits, ces aspects méritent d'être améliorés.

# 2. INTRODUCTION

Le Conseil de recherches en sciences naturelles et en génie (CRSNG) a exigé une vérification de son système informatisé de gestion des subventions et bourses (SIGSB) dans les buts suivants :

1. s'assurer que le SIGSB respecte les règles administratives améliorées nécessaires afin :
    - de garantir l'intégrité des données,
    - Gérer et suivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG,
    - Accepter et enregistrer la demande initiale,
    - Observer la sélection par les pairs,
    - Gérer les subventions post-octrois,
    - Communiquer des données;
2. s'assurer que le SIGSB comprend les contrôles nécessaires pour le suivi du financement et des paiements;
3. s'assurer que le système possède les contrôles nécessaires pour toute information financière du SIGSB transmise au SFAGAI;
4. établir la pertinence du cadre de contrôle de gestion (sujet abordé dans la conclusion générale);
5. établir l'efficacité du SIGSB en ce qui a trait à sa convivialité, l'ampleur de sa portée, etc.

Le SIGSB, une application mise au point selon les principes du Conseil du Trésor et une méthodologie orientée objets, sert à gérer et à suivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG, à enregistrer les demandes de subventions initiales, à effectuer la sélection par les pairs, à enregistrer l'approbation finale des subventions et à gérer le financement des subventions. Le SIGSB permet aussi au CRSNG de suivre l'état du financement. De plus, le système possède une interface automatisée avec le système financier d'achat et de gestion des actifs immobilisés (SFAGAI).

La délimitation de la vérification, telle que précisée par le CRSNG (vérification interne), comprend le SIGSB ainsi que l'interface avec le SFAGAI. La vérification a été effectuée pour la période du mois de mai au mois de juillet 2003. Une vérification par sondages avec échantillon a été effectuée pour les années 2001 (traitement post-octroi seulement), 2002 et 2003. La vérification par sondages traitait de trois secteurs : les programmes de partenariats de recherche, les bourse et les subventions.

La vérification a été effectuée selon la méthodologie de vérification internationale pour l'évaluation de contrôles informatiques de Deloitte & Touche LLP; il s'agit d'une démarche exhaustive axée sur le risque et mise au point en totalité par les experts en la matière de Deloitte & Touche. Cette démarche est complétée par les meilleures pratiques utilisées par des spécialistes à l'échelle internationale. En particulier, la méthodologie de propriété comprend deux programmes de vérification

pour l'évaluation : *1) contrôles informatiques généraux* et *2) contrôles des processus opérationnels*. Ainsi, les contrôles du SIGSB ont été documentés et évalués en les comparant à un cadre de contrôle rigoureux et les recommandations à l'intention du CRSNG visaient à faciliter la mise en oeuvre des mécanismes de contrôle nécessaires. La vérification comprenait des entretiens avec le personnel du CRSNG, un examen de certaines configurations de système et de certains processus manuels et la vérification par sondages des activités de contrôle identifiées.

La vérification interne a été effectuée selon la politique du Conseil du Trésor sur la vérification interne et les normes de l'institut des vérificateurs internes.

En ce qui concerne l'objectif de la vérification portant sur la convivialité et l'ampleur de la portée, quatre groupes de consultation ont été formés pour recueillir les commentaires des intervenants sur le niveau de satisfaction pour divers éléments du système. Ces consultations ont été menées avec l'aide d'une technologie de vote anonyme. Les constatations seront traitées ailleurs.

# 3. CONSTATATIONS DU VÉRIFICATEUR - CONTRÔLES DES PROCESSUS OPÉRATIONNELS

Toutes les constatations importantes du vérificateur associées aux objectifs et critères de la vérification sont décrites dans la présente section. Elles comprennent des énoncés décrivant les critères, que les attentes soient comblées ou non. Pour chaque point en litige, le rapport comprend une description de l'observation, un énoncé sur les conséquences et une recommandation. Le niveau de risque est aussi évalué. Le risque est classifié comme suit :

Risque élevé – le point en litige devrait être réglé à court terme, peut représenter un risque important
Risque moyen – le point en litige devrait être réglé, peut représenter un risque
Risque faible – risque minime ou devrait faire l'objet des meilleures pratiques

## 3.1 Objectif de la vérification :

S'assurer que le SIGSB respecte les règles administratives améliorées nécessaires afin :

- de garantir l'intégrité des données,
- de gérer et desuivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG,
- d'accepter et d'enregistrer la demande initiale,
- d'bserver la sélection par les pairs,
- de gérer les subventions post-octrois,
- de communiquer des données.

**Critère de vérification n$^{o}$ 1.1**
***Toutes les demandes sont enregistrées avec précision, au complet et selon les délais prescrits.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme; toutefois, certains points qui méritent une amélioration ont été soulevés.

Les contrôles en place comprennent :

- l'utilisation de listes de contrôle pour le traitement des subventions et des bourses pour identifier les points en litige et l'information manquante.
- des chefs d'équipe et agents de programmes (subventions et bourses) qui effectuent la vérification de l'intégrité des données.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Faible | Dans le cas du PPR, les demandes sont traitées par les adjoints des programmes du SIGSB. Les données saisies par le SIGSB ne sont pas révisées pour assurer leur exactitude et leur intégralité. Il faut toutefois remarquer qu'aucun point de litige n'est survenu lors de vérification des demandes/fichiers du PPR. (Se reporter à l'appendice A, n° 16.) | Il existe un risque que les erreurs de données ne soient pas dépistées puisque aucun mécanisme de surveillance ou d'examen ne suit l'entrée des données. | Nous recommandons la mise en oeuvre d'un procédé, où les agents de programme réviseraient les données entrées dans le SIGSB sur une base empirique afin d'assurer leur exactitude et leur intégrité. |
| Faible | Les listes de contrôle utilisées pour l'examen des demandes n'accompagnent pas toujours la demande - surtout dans le cas des bourses. Les listes de contrôle ne sont conservées que s'il existe des points en litige qui exigent un suivi. (Se reporter à l'appendice A, n° 17.) | Si les listes de contrôle de traitement de demande ne sont pas conservées dans le dossier, il n'existe pas d'éléments probants pour vérifier leur utilisation. De plus, il n'existe aucune piste de vérification si des points en litige surviennent subséquemment. | Nous recommandons que les listes de contrôle de traitement de demande soient conservées dans le dossier de la demande. |
| Faible | Plusieurs adjoints des programmes utilisent Excel ou Lotus Notes pour suivre les demandes et comme outil de rappel. (Se reporter à l'appendice A, n° 18.) | L'utilisation de systèmes parallèles signifie l'entrée en double des données et augmente le risque d'erreur et d'informations incomplètes. | Nous recommandons au CRSNG d'étudier l'utilisation de systèmes parallèles afin d'établir si cette fonctionnalité pourrait être intégrée au SIGSB.<br><br>Se reporter à la section 5. |

**Critère de vérification n° 1.2**
***Des décisions valides prises par des examinateurs qualifiés sont enregistrées de façon précise et selon les délais prescrits dans le cas de toutes les demandes.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme en ce qui a trait aux subventions et au PPR; toutefois, certains points qui méritent une amélioration ont été soulevés, en particulier pour les bourses.

Les contrôles en place comprennent :

- Dans le cas de subventions, les dossiers de concours (Excel) sont signés par les chaires des comités avant d'être téléchargés dans le SIGSB. L'exactitude du téléchargement au SIGSB est vérifiée par un agent de programme et le chiffrier électronique est signé pour indiquer qu'une vérification a été effectuée.
- Le président examine la liste des subventions et des bourses et la signe pour autoriser l'appui d'un transfert de fonds.
- Les bourses du PPR sont approuvées par un directeur (Note : Certains programmes n'exigent pas l'approbation d'un directeur).

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Dans le cas des bourses, une vérification a révélé que les chaires des comités et les agents de programme ne signent pas les chiffriers électroniques de concours. (Ce scénario n'existe pas dans le cas des subventions où la chaire du comité ou l'agent de programme signent physiquement le chiffrier électronique de concours.)<br>(Se reporter à l'appendice A, n° 9.) | L'absence d'une approbation officielle rend impossible la vérification de l'approbation des bourses par le comité et leur contrôle par l'agent de programme. | Nous recommandons que le procédé des bourses comprenne la signature officielle de la chaire du comité ainsi que celle de l'agent de programme. Même si le point de démarcation peut changer, selon le nombre de bourses disponibles, cela fournirait une piste de vérification en ce qui a trait au classement établi par le comité. Cela ferait valoir l'obligation de rendre compte. |
| Faible | Dans plusieurs cas, la vérification a révélé qu'il était difficile de distinguer les signatures dans les dossiers de concours.<br>(Se reporter à l'appendice A, n° 15.) | Les dossiers de concours risquent de ne pas comprendre l'approbation nécessaire, ce qui augmente le risque d'octrois invalides. | Nous recommandons l'utilisation d'un formulaire officiel qui comprend le nom et le titre des signataires autorisés. |

**Critère de vérification n° 1.3**
***Tous les ajouts/changements valides aux fichiers des données permanentes sont inscrits de façon intégrale, précise et selon les délais prescrits.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme; toutefois, certains points qui méritent une amélioration ont été soulevés.

Les contrôles en place comprennent :

- les normes de saisie de données sont établies selon les noms et adresses (personnes et organismes);
- la gestion des données de base, y compris celles des comités et des organismes, a été centralisée.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Faible | Il n'existe aucun examen des changements apportés aux données de base pour assurer l'exactitude de l'entrée de données, quoique des examens des données à grande échelle soient périodiquement effectués.<br><br>Dans un cas, la vérification a révélé une erreur d'entrée de données au moment de l'inscription d'un nouvel organisme (erreur de frappe dans l'adresse).<br>(Se reporter à l'appendice A, n° 19.) | Si l'entrée de données de base du SIGSB n'est pas examinée, le risque d'erreurs et de changements non détectés augmente. | Nous recommandons que les parties intéressées considèrent une révision par un organisme indépendant des changements apportés au fichier maître pour assurer l'intégrité, l'exactitude et la validité des changements apportés au SIGSB. Cette pratique pourrait être facilitée par l'utilisation d'un rapport de changement provenant du SIGSB. |

**Critère de vérification n° 1.4**
***La séparation des tâches est appropriée et l'accès au système est restreint au personnel autorisé.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | Durant la vérification de la sécurité associée aux utilisateurs finals, nous avons remarqué que l'accès pour le transfert de fonds dans le SIGSB n'est pas restreint aux utilisateurs essentiels (à titre d'exemple, les coordonnateurs de programmes et de données et certains adjoints aux programmes). Plus de 100 utilisateurs peuvent accéder au système pour transférer des fonds. La majorité de ces utilisateurs ont aussi l'accès nécessaire pour | L'accès de tous les utilisateurs au SIGSB devrait être restreint selon la fonctionnalité rattachée aux exigences du poste de l'individu. L'accès au système par de nombreux utilisateurs augmente le risque associé aux questions de séparation de tâches. En particulier, il existe un risque considérable qu'un individu puisse traiter un octroi et un transfert de fonds invalides. | Nous recommandons que les privilèges d'accès au système en service par des utilisateurs finals soient examinés afin de s'assurer que ceux-ci ne possèdent que l'accès nécessaire selon la fonctionnalité reliée à leur poste.<br><br>Si possible, nous recommandons l'amélioration du SIGSB de façon à limiter la fonctionnalité de transfert |

| | | | |
|---|---|---|---|
| | traiter des demandes, ce qui crée un risque au niveau de la séparation des tâches.<br><br>Il n'existe présentement aucun mécanisme pour limiter l'accès des utilisateurs au champ transfert sous l'onglet financement. (Se reporter à l'appendice A, n° 2.) | | de fonds (en limitant l'accès selon les champs ou en créant un nouvel onglet pour cette fonctionnalité).<br><br>Autrement, nous recommandons que l'entreprise assure la mise en oeuvre d'une surveillance ou de contrôles correctifs adéquats et efficaces pour réduire le risque à un niveau acceptable. |

**Critère de vérification n° 1.5**
***Les contrôles informatiques généraux fonctionnent de façon efficace et permettent un traitement fiable par le SIGSB.***

Se reporter à la section 4.

**3.2 <u>Objectif de la vérification</u> :**
S'assurer que le SIGSB comprend les contrôles nécessaires pour le suivi du financement et des paiements

**Critère de vérification n° 2.1**
***Tous les décaissements sont approuvés, sont calculés de façon précise et ne sont distribués que lorsque les fonds sont disponibles.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Les contrôles en place comprennent :

- Le président examine la liste des subventions et des bourses d'étude et appose sa signature pour autoriser le transfert des fonds.
- Dans le cas de plusieurs types de programme, des rapports d'étape doivent être soumis afin de conserver la subvention. Selon ce rapport et d'autres renseignements, l'agent de programme recommande si la subvention reste en vigueur ou pas et le directeur l'approuve.
- Le traitement de transferts de fonds par lots de l'étape financement à l'étape paiement, dans le cadre du SIGSB, fait l'objet d'une surveillance par le personnel de gestion afin d'assurer son exécution selon les délais prescrits, ainsi que l'examen et la résolution de toute exception. Se reporter également à la section 4.1.

**Critère de vérification n° 2.2**
***Les décaissements initiaux et continus sont corrects, sont effectués et enregistrés selon les délais prescrits et ne sont offerts qu'aux candidats qui répondent aux exigences d'acceptabilité.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme dans le cas des subventions et du PPR; toutefois, dans le cas des bourses d'étude, certains points qui méritent une amélioration ont été soulevés.

Les contrôles en place comprennent :

- Le SIGSB met automatiquement les paiements en attente sous l'onglet paiement pour les raisons suivantes :
  - changement du montant octroyé effectif sous l'onglet financement;
  - changement de l'état de l'octroi sous l'onglet financement (p. ex. fins d'octroi et transferts);
  - changements sous l'onglet financement après le transfert initial .

  La section des finances distribue manuellement les paiements en attente en vertu de pièces justificatives telles que les lettres d'approbation et les formulaires d'approbation des subventions.
- Lorsque des rapports d'étape sont nécessaires pour conserver la subvention, l'agent de programme recommande que la subvention reste en vigueur ou pas.
- Le traitement de transferts de fonds par lots de l'étape financement à l'étape paiement, dans le cadre du SIGSB, fait l'objet d'une surveillance par le personnel de gestion afin d'assurer son exécution selon les délais prescrits, ainsi que l'examen et la résolution de toute exception. Se reporter à la section 4.1.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Une vérification du procédé post-octroi a révélé que certaines universités n'avaient soumis aucune documentation au CRSNG pour confirmer l'acceptabilité du bénéficiaire de la subvention. (Se reporter à l'appendice A, n° 8.) | Un titulaire d'une subvention inadmissible pourrait continuer de recevoir des paiements. | Nous recommandons un protocole qui oblige les universités à soumettre des pièces justificatives appuyant l'admissibilité des candidats et que ce protocole soit appliqué par l'équipe post-octroi. Si les pièces justificatives ne sont pas fournies, nous recommandons le refus du financement. |

**Critère de vérification n° 2.3**
***Les affectations des fonds des programmes sont autorisées et inscrites dans le SIGSB.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Les contrôles en place comprennent :

- Le traitement de téléchargements de budgets fait l'objet d'une surveillance par le personnel de gestion afin d'assurer son exécution selon les délais prescrits, ainsi que l'examen et la résolution de toute exception. Se reporter à la section 4.1.
- Lorsqu'un utilisateur modifie un montant octroyé effectif ou offre une subvention, le SIGSB effectue automatiquement une vérification pour savoir si les fonds sont disponibles (selon les affectations de niveau 2). Cela s'applique aux programmes de subventions et au PPR. Cette vérification ne s'applique pas aux bourses puisque le nombre de bourses octroyées tient compte des abandons/fins d'octroi/etc. Il est donc possible que l'affectation des fonds soit dépassée.

**Critère de vérification n° 2.4**
***La séparation des tâches est appropriée et l'accès aux systèmes est restreint au personnel autorisé.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | Durant la vérification de la sécurité associée aux utilisateurs finals, nous avons remarqué que l'accès pour la gestion de l'information budgétaire n'est pas restreint au personnel autorisé. À titre d'exemple, 21 utilisateurs peuvent accéder aux affectations des finances du conseil, alors que seulement 3 utilisateurs devraient détenir ce privilège.<br><br>Nous avons aussi remarqué que 10 utilisateurs peuvent accéder à l'onglet financement, l'onglet paiement et le dossier de la demande.<br>(Se reporter à l'appendice A, n° 1.) | L'accès de tous les utilisateurs au SIGSB devrait être restreint selon la fonctionnalité rattachée aux exigences du poste de l'individu.<br><br>L'accès au système par de nombreux utilisateurs augmente le risque associé aux questions de séparation des tâches. Dans ce cas, un individu pourrait créer une demande, traiter le transfert des fonds et distribuer/changer les paiements. | Nous recommandons que les privilèges d'accès au système en service par des utilisateurs finals soient examinés afin de s'assurer que ceux-ci ne possèdent que l'accès nécessaire selon la fonctionnalité reliée à leur poste.<br><br>Si l'accès au système ne peut être restreint, nous recommandons que l'entreprise assure la mise en oeuvre d'une surveillance ou de contrôles correctifs adéquats et efficaces pour réduire le risque à un niveau acceptable. |

**Critère de vérification n° 2.5**
***Les contrôles informatiques généraux fonctionnent de façon efficace et permettent un traitement fiable par le SIGSB.***

Se reporter à la section 4.

**3.3 <u>Objectif de la vérification</u> :**
S'assurer que le système possède les contrôles nécessaires pour toute information financière du SIGSB transmise au SFAGAI.

**Critère de vérification n° 3.1**
***L'information sur les décaissements est transmise de façon précise et intégrale au SFAGAI selon les délais prescrits.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Les contrôles en place comprennent :

- Le programme de paiements est exécuté par un agent des finances selon une base périodique et un horaire fixe établi par la section des finances. Cette pratique assure la distribution de paiements selon les délais prescrits et l'intégrité des renseignements.
- S'il existe une erreur au niveau du programme de paiements et de l'importation vers le SFAGAI, un rapport d'erreur est produit. En cas d'erreurs, le commis des paiements de subventions effectue le suivi nécessaire. Il entre aussi en communication avec le SFAGAI pour vérifier si l'importation a été bien exécutée.
- Chaque mois, le système compare les données du SFAGAI à celles du SIGSB afin d'identifier toute information manquante. De plus, une conciliation entre le SIGSB et les relevés de compte des universités est effectuée chaque année pour identifier les divergences et effectuer le suivi nécessaire.
- Toutes les données financières sont transférées du SIGSB au SFAGAI (interface). Se reporter à la section 4.1

**Critère de vérification n$^{o}$ 3.2**
***Les contrôles informatiques généraux fonctionnent de façon efficace et permettent un traitement fiable par le SIGSB.***

Se reporter à la section 4.

# 4. CONSTATATIONS DU VÉRIFICATEUR - CONTRÔLES INFORMATIQUES GÉNÉRAUX

Toutes les constatations importantes du vérificateur liées aux objectifs et critères de la vérification sont décrites dans la présente section. Elles comprennent des énoncés décrivant les critères, que les attentes soient comblées ou non. Pour chaque point en litige, le rapport comprend une description de l'observation, un énoncé sur les conséquences et une recommandation. Le niveau de risque est aussi évalué. Le risque est classifié comme suit :

Risque élevé – le point en litige devrait être réglé à court terme, peut représenter un risque important
Risque moyen – le point en litige devrait être réglé, peut représenter un risque
Risque faible – risque minime ou devrait faire l'objet des meilleures pratiques

**4.1** **Objectif de la vérification :**
Les traitements par lots sont effectués selon les délais prescrits et de façon intégrale.

**Critère de vérification n$^{o}$ 1.1**
***Le traitement de téléchargements de budgets, de téléchargements de chiffriers électroniques et le transfert de fonds par lots de l'étape financement à l'étape paiement font l'objet d'une surveillance par le personnel de gestion afin d'assurer son exécution selon les délais prescrits, ainsi que l'analyse et la résolution de toute exception.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Même si le personnel de gestion ne surveille pas expressément ces procédés (c.-à-d., passage de l'étape financement à l'étape paiement dans le cadre du SIGSB), des activités de réconciliation sont effectuées par le personnel du CRSNG et les documents à l'appui sont conservés.

**4.2** **Objectif de la vérification :**
Seuls les programmes en service valides sont exécutés.

**Critère de vérification n$^{o}$ 2.1**
***L'accès aux programmes exécutables est restreint aux individus qui doivent exécuter, modifier, supprimer ou créer ces programmes.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | L'accès au système nécessaire pour modifier, supprimer ou créer les fichiers exécutables du SIGSB n'est pas contrôlé de façon appropriée. Présentement, 15 utilisateurs peuvent accéder au répertoire contenant les fichiers exécutables en service (c.-à-d., P:/Namis/Prod/). Deux de ces individus ne travaillent plus pour le CRSNG. (Se reporter à l'appendice A, n° 7.) | Les changements non autorisés au SIGSB peuvent entraîner des renseignements inexacts, l'utilisation inappropriée des ressources du système, et un surplus de gestion et de soutien pour corriger les problèmes de traitement. | Nous recommandons que le CRSNG limite l'accès « écriture » au répertoire P:/NAMIS/Prod à l'individu responsable de la migration de programmes au système en service, ainsi qu'à son remplaçant autorisé. Cette pratique réduira la possibilité de changements non autorisés au SIGSB. |
| Moyen | L'accès au système nécessaire pour exécuter les programmes par lots du SIGSB n'est pas contrôlé de façon appropriée. À titre d'exemple, parmi les 13 utilisateurs capables d'exécuter le transfert par lots du financement des subventions à l'étape paiement et les 9 utilisateurs capables d'exécuter le transfert par lots du financement des bourses à l'étape paiement, seulement 2 individus peuvent justifier ce privilège d'accès. (Se reporter à l'appendice A, n° 10.) | Les privilèges non justifiés pour le traitement par lots dans le SIGSB mettent en jeu l'intégrité de l'information corporative. | Nous recommandons que l'accès nécessaire pour télécharger les chiffriers électroniques de concours et le transfert par lots des fonds de l'étape financement à l'étape paiement dans le SIGSB soit restreint aux individus qui en ont réellement besoin pour effectuer leurs tâches. |

**4.3** **Objectif de la vérification :**
Toutes les données financières sont transférées du SIGSB au SFAGAI (interface).

**Critère de vérification n° 3.1**
***Les contrôles sont en place pour assurer que les transferts de données au SFAGAI sont traités de façon intégrale.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Il existe des contrôles de réconciliation adéquats pour le téléchargement des paiements au SFAGAI, ainsi que des documents à l'appui et un suivi dans le cas d'exceptions.

**4.4** **Objectif de la vérification :**
Des outils et des techniques de sécurité logique sont élaborés et configurés afin de restreindre l'accès au SIGSB.

**Critère de vérification n° 4.1**
***Des outils et des techniques de sécurité des données sont utilisés pour restreindre l'accès aux ressources du SIGSB (p. ex., fichiers de données, utilitaires, transactions, programmes).***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

L'utilitaire de sécurité du SIGSB permet de contrôler l'accès au niveau de l'onglet, du rapport, de l'utilitaire (c.-à-d., transferts par lots de l'étape financement à l'étape paiement et téléchargements des chiffriers électroniques).

**4.5** **Objectif de la vérification :**
Les outils et des techniques de sécurité logique sont gérés de façon à restreindre l'accès aux programmes, aux données et à certaines autres ressources informationnelles du SIGSB.

**Critère de vérification n° 5.1**
***Les propriétaires d'application autorisent le genre de privilèges d'accès des utilisateurs et leur ampleur, et ces privilèges seront examinés par les propriétaires pour assurer leur pertinence.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Même s'il existe un procédé par lequel les propriétaires des ressources informationnelles peuvent autoriser l'accès aux utilisateurs, la piste de vérification est inadéquate. À titre d'exemple, les propriétaires des ressources informationnelles ne précisent pas l'accès à « onglets/rapports/utilitaires/programmes », mais spécifient plutôt « accorder lui le même accès que l'utilisateur X ... ». Puisque l'accès accordé à X n'est pas inscrit sur le formulaire, il est | Le procédé utilisé pour accorder les privilèges d'accès est imparfait et l'examen des privilèges d'accès par les propriétaires des ressources informationnelles n'est pas effectué régulièrement. Cela met à risque les actifs de l'organisme et l'intégrité de l'information corporative. | Nous recommandons que les propriétaires des ressources informationnelles du CRSNG autorisent l'accès au niveau de l'onglet, du rapport, de l'utilitaire et du programme. De plus, les propriétaires des ressources informationnelles devraient régulièrement réexaminer les privilèges d'accès.<br><br>Nous recommandons aussi qu'un lien soit établi avec la section des ressources |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| | impossible de vérifier si les privilèges accordés sont les mêmes que ceux que le propriétaire des ressources informationnelles a approuvé lorsque le formulaire a été rempli.<br><br>Nous avons aussi remarqué que la pertinence de l'accès accordé aux utilisateurs n'est pas examinée régulièrement par les propriétaires des ressources informationnelles.<br><br>De plus, les privilèges d'accès ont été vérifiés pour un groupe de 15 utilisateurs; dans certains cas, il était exagéré. À titre d'exemple, 3 utilisateurs du secteur des finances du groupe possèdaient des privilèges au-delà des exigences de leurs tâches.<br>(Se reporter à l'appendice A, n° 11.) | | humaines afin de s'assurer que les privilèges d'accès sont mis à jour ou supprimés selon le cas lorsqu'un utilisateur part ou qu'il est muté. |

**4.6** **Objectif de la vérification :**
Des contrôles d'accès physique sont mis en oeuvre et gérés afin de s'assurer que seulement les individus autorisés peuvent accéder aux ressources informationnelles ou les utiliser.

**Critère de vérification n° 6.1**
***L'accès physique à l'édifice, et aux alentours où se trouvent les ordinateurs, est surveillé et restreint aux individus qui en ont besoin pour effectuer leurs tâches.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme; toutefois, certains points qui méritent une amélioration ont été soulevés.

Les contrôles en place comprennent :

- L'accès à la salle des ordinateurs par le personnel du CRSNG et du CRSH semble bien contrôlé (seulement 7 membres du personnel de technologie de l'information possèdent un privilège d'accès continu et un employé contractuel possède un privilège d'accès de 08h00 à 17h00).

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Faible | Le CRSNG et le CRSH partagent la salle des ordinateurs avec le Conseil des arts du Canada. Le CRSNG n'exerce aucun contrôle sur les membres du personnel du Conseil des arts du Canada qui peuvent accéder à la salle des ordinateurs. (Se reporter à l'appendice A, n° 20.) | Les ressources informationnelles du CRSNG comprennent le matériel informatique, les périphériques, des supports de données et la documentation des systèmes informatiques. L'accès physique à de telles ressources permet à l'utilisateur de visionner, d'utiliser, d'endommager ou de détourner ces ressources. | Nous recommandons que l'accès aux ressources informationnelles du CRSNG et du CRSH soit restreint à leurs propres membres du personnel autorisés. |

**4.7** **Objectif de la vérification :**
Les ressources informationnelles sont protégées contre les risques environnementaux et les dommages connexes.

**Critère de vérification n° 7.1**
***Le personnel de gestion surveille périodiquement l'efficacité des systèmes de contrôle des conditions ambiantes et évalue les répercussions sur les opérations des menaces potentielles pour les ressources informationnelles.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme. Certaines améliorations sont présentement en cours.

La salle des ordinateurs est présentement dotée de régulateurs de température surveillés par Honeywell, de deux refroidisseurs à l'eau pour refroidir la salle, de détecteurs d'humidité, de blocs d'alimentation électrique sans interruption, de gicleurs à eau et de planchers surélevés. La DSI travaille présentement à l'amélioration de la sécurité physique et du contrôle des conditions ambiantes des ressources informationnelles. Nous avons étudié les bons de commande pour le nettoyage de la salle des ordinateurs et des placards de câblage, la surveillance des conditionneurs d'air, l'achat et l'installation des caméras de sécurité, et la surveillance et l'entretien des caméras.

**4.8** **Objectif de la vérification :**
Les politiques et les procédures pour l'administration complète et la mise en oeuvre de la sécurité informatique sont documentées.

**Critère de vérification n° 8.1**
***Les politiques de sécurité informatique sont officiellement documentées et transmises aux utilisateurs, et ces politiques sont surveillées pour en assurer la conformité et examinées régulièrement.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Les politiques de sécurité associées au SIGSB sont documentées dans la politique du Conseil sur l'utilisation permise des réseaux électroniques, le guide de sécurité du SIGSB et la documentation sur les trois rôles de gestion du SIGSB (Consignataire des données, Coordonnateur, gestion des données et Gardien des données). Un nouveau comité directeur et un groupe de travail sur la sécurité ont récemment été formés.

**Critère de vérification n$^{o}$ 8.2**
***Les utilisateurs du SIGSB doivent signer un formulaire attestant qu'ils ont lu les politiques portant sur la sécurité informatique et qu'ils s'engagent à les respecter.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Les points en litige sont les suivants :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Même s'il existe un formulaire qui permet aux employés d'apposer leur signature en guise d'approbation de la politique du Conseil sur l'utilisation permise des réseaux électroniques, son utilisation n'a pas été prescrite et la majorité des employés ne l'ont pas signé.<br>(Se reporter à l'appendice A, n$^{o}$ 13.) | Il existe un risque considérable que les utilisateurs ne comprennent pas la politique sur l'utilisation permise des réseaux électroniques, ou ne s'y conforment pas. Si les utilisateurs ne sont pas obligés de lire la politique, et de signer le formulaire, il devient difficile pour le CRSNG de l'appliquer. | Nous recommandons que la responsabilité pour la mise en oeuvre de ce procédé soit clairement identifiée et que l'individu responsable effectue le suivi nécessaire afin que le dossier de tous les employés contienne un formulaire signé sur l'utilisation des réseaux électroniques. |

**4.9 Objectif de la vérification :**
En cas de désastre, les systèmes informatiques et les processus opérationnels essentiels peuvent être récupérés en peu de temps.

**Critère de vérification n$^{o}$ 9.1**
***Des outils de rétention automatique des données sont disponibles pour gérer le plan et le calendrier de la procédure de sauvegarde et de rétention des données.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

La DSI utilise une bibliothèque de rubans Legato pour gérer les sauvegardes du SIGSB. Une sauvegarde complète des données SIGSB est effectuée chaque jour.

**Critère de vérification n$^{o}$ 9.2**
***Le personnel de gestion examine périodiquement l'état des sauvegardes pour assurer leur conformité aux plans et calendriers de sauvegarde et de rétention des données.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Un analyste technique en chef de la DSI examine le registre de sauvegardes chaque jour pour s'assurer que les sauvegardes de la veille sont intègres.

**Critère de vérification n° 9.3**
***Les sauvegardes sont archivées hors site pour minimiser le risque de perte de données.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Tel que l'ont confirmé nos discussions avec le personnel de la DSI, les rubans sont entreposés hors site (Archives nationales du Canada). Nous avons obtenu un reçu de livraison pour un ruban de sauvegarde du CRSNG qui provenait de l'emplacement hors site.

**Critère de vérification n° 9.4**
***Tous les supports de données (rubans, manuels, guides, etc.) sont entreposés dans un endroit sécuritaire où les conditions ambiantes sont contrôlées.***

D'après les procédés examinés et les sondages effectués, nous étions incapables d'établir si le système répondait aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Nous n'avons trouvé aucun contrat attestant que les conditions ambiantes de l'emplacement d'entreposage des rubans de sauvegarde étaient contrôlées, et aucun membre du personnel du CRSNG n'a visité cet emplacement depuis deux ou trois ans.<br>(Se reporter à l'appendice A, n° 14.) | Les causes de dommages aux ressources informationnelles peuvent être nombreuses : chaleur, fumée, feu, humidité, inondation, tremblement de terre et panne électrique. Si les ressources informationnelles ne sont pas adéquatement protégées, elles risquent de ne pas être disponibles quand elles le doivent et, en cas d'urgence, la récupération de ces ressources peut être retardée. | Nous recommandons de modifier le contrat afin de permettre au CRSNG d'effectuer régulièrement une vérification, ou d'obtenir la garantie d'un tiers, des contrôles utilisés à l'emplacement d'entreposage hors site. |

**Critère de vérification n° 9.5**
***La lisibilité des sauvegardes et des données retenues est vérifiée périodiquement par le biais de la restauration ou d'autres méthodes.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

**4.10 Objectif de la vérification :**

La mise en oeuvre du SIGSB est effectuée de façon adéquate et celui-ci fonctionne conformément aux attentes du personnel cadre, et toutes les modifications nécessaires du SIGSB sont effectuées selon les délais prescrits.

**Critère de vérification n° 10.1**

***Les modifications du SIGSB ont été vérifiées selon le plan d'évaluation qui comprend, comme il convient, l'essai du système et de l'unité, l'essai d'interface, l'essai en parallèle, l'essai de capacité et l'essai d'acceptation par l'utilisateur.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | Dans le cas d'essais du SIGSB, les résultats et les procédures d'essai ne sont pas officiellement documentés. Le personnel de l'assurance de la qualité effectue des essais et imprime les résultats, mais il n'existe aucun calendrier pour la rétention des résultats. (Se reporter à l'appendice A, n° 12) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux changements récemment implémentés dans le SIGSB en raison de la portée trop restreinte des essais. L'approbation officielle des utilisateurs leur transmet un sentiment d'appartenance afin d'assurer l'exécution des essais nécessaires. | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Une fois les essais préétablis terminés, les utilisateurs devraient apposer leur signature pour officiellement approuver les changements ou les améliorations apportés au système. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au moment de la mise en oeuvre d'un changement au système ou à une application. Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |

**Critère de vérification n° 10.2**

***Les demandes de modification, y compris les mises à jour et les corrections, du SIGSB provenant des utilisateurs et d'autres sources, sont approuvées par le personnel de cadre et mises en oeuvre si elles sont compatibles avec les plans de systèmes informatiques et les intentions du personnel cadre.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Même si le SIGSB est doté d'un procédé de gestion du changement approprié, qui intègre l'approbation et l'établissement des priorités pour les changements par le groupe des utilisateurs du SIGSB, il n'est pas respecté de façon uniforme par les développeurs.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | Même si le SIGSB est doté d'un procédé de gestion du changement approprié, il n'est pas respecté de façon uniforme par les développeurs. Sur 6 modifications apportées au code source du SIGSB, seulement 4 possédaient un renvoi croisé au système Rational ClearQuest, lequel indiquait l'approbation du personnel cadre. (Se reporter à l'appendice A, n° 4.) | Le manque de procédés officiels et de documentation pourrait entraîner la mise en oeuvre de changements non autorisés ou de changements qui ne répondent pas aux attentes des utilisateurs ou du personnel cadre. De plus, l'entretien éventuel, y compris la résolution de problèmes, de l'application utilisée risque d'être plus difficile. | Nous recommandons que le personnel cadre s'assure que le procédé de gestion du changement soit respecté et qu'il soit utilisé de façon uniforme par les développeurs. |

**4.11 Objectif de la vérification :**

Les logiciels de réseau et de communication sont mis en oeuvre de façon appropriée et fonctionnent selon les intentions du personnel cadre et les modifications intégrées à ces logiciels sont effectuées selon les délais prescrits.

**Critère de vérification n° 11.1**

***Les nouveaux logiciels de réseau et de communication et les modifications connexes sont vérifiés selon le plan d'évaluation qui comprend, comme il convient, l'essai du système et de l'unité, l'essai d'interface, l'essai en parallèle, l'essai de capacité et l'essai d'acceptation par l'utilisateur.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | L'essai des modifications apportées aux logiciels de réseau et de communication n'est pas effectué de façon officielle et n'est pas documenté. (Se reporter à l'appendice A, n° 5.) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux modifications récentes apportées aux logiciels de | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au |

| | | | |
|---|---|---|---|
| | | réseau et de communication du SIGSB en raison de la portée trop restreinte des essais. | moment des modifications apportées aux logiciels de réseau et de communication du SIGSB. Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |

**Critère de vérification n$^{o}$ 11.2**
***Les demandes de modification, y compris les mises à jour et les corrections, des logiciels d'infrastructure de réseau et de communication provenant des utilisateurs et d'autres sources, sont approuvées par le personnel cadre et mises en oeuvre si elles sont compatibles avec les plans de systèmes informatiques et les intentions du personnel cadre.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | Aucun procédé de gestion du changement officiellement documenté n'est utilisé pour traiter des changements apportés aux logiciels de réseau et de communication du SIGSB. Les demandes de changement ne sont pas traitées de façon officielle et il n'existe aucun procédé officiel d'approbation. Puisque les modifications ne sont pas enregistrées, il est impossible de vérifier si tous les changements ont été approuvés par le personnel cadre.<br>(Se reporter à l'appendice A, n$^{o}$ 3.) | Le manque de procédés officiels et de documentation portant sur les changements apportés aux logiciels de réseau et de communication pourrait entraîner la mise en oeuvre de changements non autorisés ou de changements qui ne répondent pas aux attentes des utilisateurs ou du personnel cadre. De plus, sans documentation adéquate, l'entretien éventuel, y compris la résolution de problèmes, des logiciels de réseau et de communication risque d'être plus difficile. | Nous recommandons d'officialiser le procédé de gestion du changement, et d'utiliser des formulaires de demandes de changement selon les politiques et procédures pertinentes. De plus, nous recommandons que les documents d'approbation soient conservés afin de servir de référence et d'établir une piste de vérification. |

**4.12** **<u>Objectif de la vérification</u> :**
Les logiciels de base sont mis en oeuvre de façon appropriée et fonctionnent selon les intentions du personnel cadre et les modifications intégrées à ces logiciels sont effectuées selon les délais prescrits.

**Critère de vérification n° 12.1**
***Les nouveaux logiciels de base et les modifications connexes sont vérifiés selon le plan d'évaluation qui comprend, comme il convient, l'essai du système et de l'unité, l'essai d'interface, l'essai en parallèle, l'essai de capacité et l'essai d'acceptation par l'utilisateur.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | L'essai des modifications apportées aux logiciels de base n'est pas effectué de façon officielle et n'est pas documenté. (Se reporter à l'appendice A, n° 6.) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux modifications récentes des logiciels de base du SIGSB en raison de la portée trop restreinte des essais. | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au moment des modifications apportées aux logiciels de base du SIGSB. Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |

**Critère de vérification n° 12.2**
***Les demandes de modification apportées aux logiciels de base (distribués par les fournisseurs), y compris les mises à jour et les corrections, provenant des utilisateurs et d'autres sources, sont approuvées par le personnel cadre et mises en oeuvre si elles sont compatibles avec les plans de systèmes informatiques et les intentions du personnel cadre.***

D'après les procédés examinés et les sondages effectués, le système ne répond PAS aux exigences de la norme.

Le point en litige est le suivant :

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | Aucun procédé de gestion du changement officiellement documenté n'est utilisé pour traiter des changements apportés | Le manque de procédés officiels et de documentation portant sur les changements apportés aux logiciels de base | Nous recommandons de rendre officiel le procédé de gestion du changement, et d'utiliser des formulaires de |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| | aux logiciels de base du SIGSB. Les demandes de changement ne sont pas traitées de façon officielle et il n'existe aucun procédé officiel d'approbation. Puisque les modifications ne sont pas enregistrées, il est impossible de vérifier si tous les changements ont été approuvés par le personnel cadre. (Se reporter à l'appendice A, n° 3.) | pourrait entraîner la mise en oeuvre de changements non autorisés ou de changements qui ne répondent pas aux attentes des utilisateurs ou du personnel cadre. De plus, sans documentation adéquate, l'entretien éventuel, y compris la résolution de problèmes, des logiciels de base risque d'être plus difficile. | demandes de changement selon les politiques et procédures pertinentes. De plus, nous recommandons que les documents d'approbation soient conservés afin de servir de référence et d'établir une piste de vérification. |

**4.13** **Objectif de la vérification :**
Les stratégies, les plans et les budgets des systèmes informatiques sont compatibles avec les objectifs et la stratégie de l'organisme.

**Critère de vérification n° 13.1**
***Les stratégies et les plans, à long et à court terme, des systèmes informatiques ont été mis au point par le personnel cadre pour appuyer la stratégie générale de l'entreprise et les exigences des systèmes informatiqes. La performance des systèmes informatiques est surveillée par le personnel cadre en fonction des plans à long et à court terme.***

D'après les procédés examinés et les sondages effectués, le système répond aux exigences de la norme.

Le rapport annuel de la DSI à l'intention du CRSNG comprend de l'information budgétaire et des plans. Les réunions du groupe des utilisateurs du SIGSB traitent de la planification du SIGSB.

**4.14** **Objectif de la vérification :**
Le niveau de service offert par les fournisseurs d'impartition répond aux attentes du personnel cadre, ou les dépasse.

**Critère de vérification n° 14.1**
***Le personnel cadre surveille le niveau de service des systèmes informatiques et prend les mesures correctives nécessaires si la performance n'est pas à la hauteur.***

D'après les procédés examinés et les sondages effectués, cette norme ne s'applique pas au CRSNG.

Selon le gestionnaire de projet de la DSI, aucune fonction principale liée à la technologie de l'information n'est offerte en impartition. Selon le conseiller en élaboration de projets, le gestionnaire de projet, DSI, le gestionnaire des services techniques et le coordonnateur de la sécurité des technologies de l'information, dans le cas de petits contrats, tels que ceux avec les experts-conseils, les politiques du Conseil du Trésor s'appliquent.

# 5. CONSTATATIONS - CONVIVIALITÉ / AMPLEUR DE LA PORTÉE

**5.1 Objectif de la vérification :**
Établir l'efficacité du SIGSB en tenant compte de sa convivialité, de l'ampleur de sa portée, etc.

Afin d'analyser la convivialité et l'ampleur de la portée du SIGSB, nous avons établi une liste de critères d'évaluation clé (expérience de l'utilisateur, fonctionnalité, architecture de système et aide et soutien), nous avons formé des groupes de discussion avec les utilisateurs et avons obtenu le résultat des sondages et de l'information qualitative portant sur l'opinion des utilisateurs sur les critères établis.

Pour faciliter le processus, les utilisateurs ont formé des groupes de discussion selon les catégories suivantes :

| Groupe | Description |
|---|---|
| Utilisateurs du SIGSB | Les membres du groupe des utilisateurs du SIGSB qui interviennent à différentes étapes. Le groupe des utilisateurs du SIGSB s'occupe d'établir la priorité des changements et sert d'interface entre la DSI et les utilisateurs. |
| Grands utilisateurs | Ce groupe comprend ceux qui utilisent le SIGSB quotidiennement. |
| Faibles utilisateurs | Ce groupe, composé surtout de gestionnaires, comprend ceux qui utilisent le SIGSB occasionnellement - habituellement pour consulter les données ou en communiquer. |
| Utilisateurs experts | Ce groupe comprend des membres de la DSI et de l'équipe des Affaires électroniques. |

**Expérience de l'utilisateur**
*Constatations générales :*

- Le groupe des grands utilisateurs était celui qui avait le plus de réserve en ce qui concerne la convivialité du SIGSB. Les préoccupations principales étaient liées à la réactivité, à la capacité de demander des renseignements et à la capacité de modifier l'application selon les tâches et les départements spécifiques.
- Lors de l'analyse de l'information selon les secteurs d'activités des intervenants, nous avons remarqué que les utilisateurs provenant des secteurs subventions et du PPR étaient ceux qui ressentaient le plus le besoin d'améliorer le système. Le personnel des finances et du PPR se préoccupait de la personnalisation et ressentait que le système était conçu pour un seul secteur d'activités (c.-à-d. celui des subventions et des bourses) et qu'une personnalisation supplémentaire ou des modifications pour les divers départements seraient de mise pour améliorer la convivialité du SIGSB.

*Recommandations :*
Le CRSNG devrait considérer la possibilité de traitement des rapports en arrière-plan qui permettrait l'utilisation concomitante de l'application pendant la préparation des rapports. Cela pourrait améliorer la productivité des utilisateurs.

Nous recommandons aussi que le CRSNG envisage de modifier le SIGSB afin d'intégrer des écrans pour l'utilisation spécifique de certains départements. Cela faciliterait l'utilisation de l'application pour chaque département en créant des écrans supplémentaires plus pertinents et intuitifs, conçus selon leurs exigences particulières.

Ces deux recommandations, qui doivent être appuyées par une analyse coûts-avantages et les priorités établies, constituent les aspects les plus importants de l'analyse effectuée pour cette catégorie.

**Fonctionnalité**

*Constatations générales :*

- Tous les groupes ressentaient que le SIGSB pouvait être doté d'outils et de procédures manuelles supplémentaires pour complémenter les procédures quotidiennes. Notamment, les groupes des grands et faibles utilisateurs trouvaient que certaines procédures manuelles pouvaient être automatisées. En ce qui a trait à l'intégration, la majorité des utilisateurs était satisfaite du niveau d'intégration interne du SIGSB.
- Parmi les unités d'entreprise, le personnel du PPR se préoccupait plus de la fonctionnalité. En grande partie, les commentaires étaient liés à la communication de données dans le SIGSB, ainsi qu'aux systèmes et processus externes nécessaires pour compléter le dossier des candidats et pour fournir des statistiques et l'analyse de l'information.

*Recommandations :*

Selon l'analyse effectuée, il existe de nombreux secteurs fonctionnels qui ne sont pas traités par les applications existantes. Les exigences établies dans le domaine de gestion des intervenants sont liées aux interactions de gestion, aux demandes, à la rétroaction, aux appels, aux visites de sites, aux promotions, à la prospection et aux conférences. Même si la conception du SIGSB n'incluait pas ces articles, le système ne semble pas répondre aux exigences de l'entreprise dans ce secteur. Nous recommandons que le CRSNG envisage d'ajouter à son plan stratégique la mise en oeuvre d'un outil pour la gestion des relations avec la clientèle pour appuyer une fonctionnalité qui n'est pas actuellement présente dans le SIGSB.

L'utilisation d'outils pour la gestion des relations avec la clientèle devient de plus en plus populaire auprès des organismes subventionnaires qui veulent complémenter ou remplacer les systèmes opérationnels. L'utilisation d'une application commerciale standard permettrait à l'organisme de réduire le risque associé aux projets de développement d'applications personnalisées et au CRSNG de rester à la fine pointe des technologies sans investissement important de la part du groupe interne de technologie de l'information. Au besoin, ce type d'outils peut servir de point de départ pour les initiatives du CRSNG en matière de commerce électronique. L'analyse complète de cette option devrait être considérée, mais doit être appuyée par une analyse de rentabilisation et un examen des priorités corporatives.

**Architecture de système**

*Constatations générales :*

- Sauf dans le cas de la stabilité du système, considérée satisfaisante par tous les utilisateurs, le niveau de satisfaction variable parmi les divers groupes de discussion était très important pour cette catégorie.
- Parmi les résultats des diverses unités d'entreprise, le groupe des subventions se distinguait par ses préoccupations substantielles. Tous les autres groupes, sauf la DSI et Autres (surtout des utilisateurs experts) se préoccupaient de la flexibilité et de l'adaptabilité du système et de l'efficacité du processus du contrôle des changements.

*Recommandations :*

Nous recommandons que le CRSNG examine les processus actuels utilisés pour évaluer et établir la priorité des changements demandés par les utilisateurs. Les réponses des intervenants indiquent qu'il existe des occasions potentielles d'améliorer le processus utilisé pour établir les priorités, ou à tout le moins, les cotes des groupes de discussion indiquent que les utilisateurs ont besoin d'explications supplémentaires sur les décisions prises dans le contexte des autres initiatives et priorités du CRSNG.

**Aide et soutien**

*Constations générales :*

- La majorité des intervenants ont favorablement accueilli l'assistance en ligne pour les utilisateurs et les manuels des procédures. Certains se préoccupaient de savoir si les renseignements étaient à jour; toutefois, peu d'utilisateurs se reportaient aux guides ou aux fonctions d'aide et préféraient consulter des collègues ou la DSI.
- Le programme de formation intiale a aussi bien été coté par les groupes. Chaque utilisateur doit effectuer une révision structurée de l'application et des guides des procédures avant de commencer son travail. Les utilisateurs ont toutefois noté qu'une formation subséquente leur permettrait d'exploiter les fonctions des applications de façon plus efficace et d'utiliser le système de façon consistante pour toutes les étapes. On a suggéré que des séances de formation intermédiaire et avancée ou des rencontres moins encadrées pour discuter de nouveaux sujets seraient utiles.

*Recommandations :*
Nous recommandons que le CRSNG examine son programme de formation continue et son curriculum en raison des remarques faites par les utilisateurs qui ressentaient le besoin de formation supplémentaire. Il faudrait considérer l'ajout au programme de séances de formation portant sur la fonctionnalité avancée ou de rencontres moins structurées pour discuter de nouveaux sujets. Ces rencontres devraient inclure un groupe d'utilisateurs, et non avec seulement un individu, pour encourager l'échange de renseignements et la livraison de messages consistants à tous les utilisateurs.

Se reporter à l'appendice C pour une vue d'ensemble des résultats de l'analyse de la convivialité et de l'ampleur de la portée.

# 6. CONCLUSION

Nous avons conclu que, alors que les contrôles des processus opérationnels appuient adéquatement les objectifs de la vérification, les contrôles informatiques généraux de certains secteurs ne semblent pas appuyer de façon efficace le traitement du SIGSB. De plus, il existe des risques associés à l'accès au SIGSB et à la séparation des tâches. Malgré la présence de certaines forces, nous avons conclu que l'ensemble du cadre de contrôle n'est pas adéquat en raison des risques identifiés.

**Les contrôles d'application (processus opérationnel)** appuient adéquatement les objectifs suivants :

1. Le SIGSB respecte les règles administratives améliorées nécessaires afin :
    - de garantir l'intégrité des données,
    - de gérer et de suivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG,
    - d'accepter et d'enregistrer la demande initiale,
    - d'observer la sélection par les pairs,
    - de gérer les subventions post-octrois,
    - de communiquer des données.
2. Le SIGSB comprend les contrôles nécessaires pour le suivi du financement et des paiements.
3. Le système possède les contrôles nécessaires pour toute information financière du SIGSB transmise au SFAGAI.

Il existe toutefois un risque en matière de sécurité et de séparation des tâches. En particulier, il est possible qu'une demande invalide soit traitée ou qu'un paiement non autorisé soit distribué en raison des contrôles inadéquats actuels. Même si notre vérification n'a pas réussi à identifier de tels cas, une vérification plus poussée serait nécessaire pour atteindre un niveau de confiance plus élevé compte tenu des risques non atténués associés aux contrôles.

**Les contrôles informatiques généraux** ne semblent pas appuyer de façon efficace les objectifs de contrôle mentionnés ci-dessus, surtout dans les secteurs de sécurité logique et de changement, et de la gestion de l'application ou du système. En particulier, il risque d'y avoir des changements non autorisés aux applications et au système, des modifications qui ne fonctionnent pas tel que prévu ou un accès non autorisé au système qui pourrait nuire au traitement du SIGSB.

Nous croyons qu'il y a lieu de grandement améliorer les contrôles internes dans les secteurs de sécurité logique et de développement et d'entretien des applications et du système.

En ce qui a trait à **la convivialité et à l'ampleur de la portée du SIGSB**, nous avons conclu que, malgré le fait que les utilisateurs sont de façon générale satisfaits du SIGSB, ces aspects du système peuvent être améliorés.

Selon notre jugement professionnel, les procédures de vérification appropriées ont été effectuées et des preuves suffisantes ont été recueillies pour appuyer les conclusions du présent rapport. Les conclusions sont fondées sur une comparaison des situations existantes au moment de la vérification par rapport aux critères de vérification. Les conclusions ne s'appliquent qu'au CRSNG.

La vérification interne a été effectuée selon la politique du Conseil du Trésor sur la vérification interne et les normes de l'Institut des vérificateurs internes pour la Pratique professionnelle de la vérification interne.

***APPENDICE A***

# PLAN D'ACTION DU PESONNEL CADRE

Résumé des observations, des conséquences et des recommandations selon le classement de risque.

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | 1. Durant la vérification de la sécurité associée aux utilisateurs finals, nous avons remarqué que l'accès pour la gestion de l'information budgétaire n'est pas restreint au personnel autorisé. À titre d'exemple, 21 utilisateurs peuvent accéder aux affectations des finances du conseil, alors que seulement 3 utilisateurs devraient détenir ce privilège.<br><br>Nous avons aussi remarqué que 10 utilisateurs peuvent accéder à l'onglet financement, l'onglet paiement et le dossier de la demande.<br>(Se reporter à la page 7.) | L'accès de tous les utilisateurs au SIGSB devrait être restreint selon la fonctionnalité rattachée aux exigences du poste de l'individu.<br><br>L'accès au système par de nombreux utilisateurs augmente le risque associé aux questions de séparation des tâches. Dans ce cas, un individu pourrait créer une demande, traiter le transfert des fonds et distribuer/changer les paiements. | Nous recommandons que les privilèges d'accès au système en service par des utilisateurs finals soient examinés afin de s'assurer que ceux-ci ne possèdent que l'accès nécessaire selon la fonctionnalité reliée à leur poste.<br><br>Si l'accès au système ne peut être restreint, nous recommandons que l'entreprise assure la mise en oeuvre d'une surveillance ou de contrôles correctifs adéquats et efficaces pour réduire le risque à un niveau acceptable. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | 2. Durant la vérification de la sécurité associée aux utilisateurs finals, nous avons remarqué que l'accès pour le transfert de fonds dans le SIGSB n'est pas restreint aux utilisateurs essentiels (à titre d'exemple, les coordonnateurs de programmes et de données et certains adjoints aux programmes). Plus de 100 utilisateurs peuvent accéder au système pour transférer des fonds. La majorité de ces utilisateurs ont aussi l'accès nécessaire pour traiter des demandes, ce qui crée un risque au niveau de la séparation des tâches.<br><br>Il n'existe présentement aucun mécanisme pour limiter l'accès des utilisateurs au champ transfert sous l'onglet financement.<br>(Se reporter à la page 5.) | L'accès de tous les utilisateurs au SIGSB devrait être restreint selon la fonctionnalité rattachée aux exigences du poste de l'individu. L'accès au système par de nombreux utilisateurs augmente le risque associé aux questions de séparation de tâches. En particulier, il existe un risque considérable qu'un individu puisse traiter un octroi et un transfert de fonds invalides. | Nous recommandons que les privilèges d'accès au système en service par des utilisateurs finals soient examinés afin de s'assurer que ceux-ci ne possèdent que l'accès nécessaire selon la fonctionnalité reliée à leur poste.<br><br>Si possible, nous recommandons l'amélioration du SIGSB de façon à limiter la fonctionnalité de transfert de fonds (en limitant l'accès selon les champs ou en créant un nouvel onglet pour cette fonctionnalité).<br><br>Autrement, nous recommandons que l'entreprise assure la mise en oeuvre d'une surveillance ou de contrôles correctifs adéquats et efficaces pour réduire le risque à un niveau acceptable. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | 3. Aucun procédé de gestion du changement officiellement documenté n'est utilisé pour traiter des changements apportés aux logiciels de réseau et de communication du SIGSB. Les demandes de changement ne sont pas traitées de façon officielle et il n'existe aucun procédé officiel d'approbation. Puisque les modifications ne sont pas enregistrées, il est impossible de vérifier si tous les changements ont été approuvés par le personnel cadre.<br>(Se reporter aux pages 15 et 16.) | Le manque de procédés officiels et de documentation portant sur les changements apportés aux logiciels de réseau et de communication pourrait entraîner la mise en oeuvre de changements non autorisés ou de changements qui ne répondent pas aux attentes des utilisateurs ou du personnel cadre. De plus, sans documentation adéquate, l'entretien éventuel, y compris la résolution de problèmes, des logiciels de réseau et de communication risque d'être plus difficile. | Nous recommandons d'officialiser le procédé de gestion du changement, et d'utiliser des formulaires de demandes de changement selon les politiques et procédures pertinentes. De plus, nous recommandons que les documents d'approbation soient conservés afin de servir de référence et d'établir une piste de vérification. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Élevé | 4. Même si le SIGSB est doté d'un procédé de gestion du changement approprié, il n'est pas respecté de façon uniforme par les développeurs. Sur 6 modifications apportées au code source du SIGSB, seulement 4 possédaient un renvoi croisé au système Rational ClearQuest, lequel indiquait l'approbation du personnel cadre.<br>(Se reporter à la page 14.) | Le manque de procédés officiels et de documentation pourrait entraîner la mise en oeuvre de changements non autorisés ou de changements qui ne répondent pas aux attentes des utilisateurs ou du personnel cadre. De plus, l'entretien éventuel, y compris la résolution de problèmes, de l'application utilisée risque d'être plus difficile. | Nous recommandons que le personnel cadre s'assure que le procédé de gestion du changement soit respecté et qu'il soit utilisé de façon uniforme par les développeurs. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Élevé | 5. L'essai des modifications apportées aux logiciels de réseau et de communication n'est pas effectué de façon officielle et n'est pas documenté.<br>(Se reporter à la page 15.) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux modifications récentes apportées aux logiciels de réseau et de communication du SIGSB en raison de la portée trop restreinte des essais. | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au moment des modifications apportées aux logiciels de réseau et de communication du SIGSB. Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Élevé | 6. L'essai des modifications apportées aux logiciels de base n'est pas effectué de façon officielle et n'est pas documenté.<br>(Se reporter à la page 16.) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux modifications récentes des logiciels de base du SIGSB en raison de la portée trop restreinte des essais. | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au moment des modifications apportées aux logiciels de base du SIGSB. Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Élevé | 7. L'accès au système nécessaire pour modifier, supprimer ou créer les fichiers exécutables du SIGSB n'est pas contrôlé de façon appropriée. Présentement, 15 utilisateurs peuvent accéder au répertoire contenant les fichiers exécutables en service (c.-à-d., P:/Namis/Prod/). Deux de ces individus ne travaillent plus pour le CRSNG.<br>(Se reporter à la page 9.) | Les changements non autorisés au SIGSB peuvent entraîner des renseignements inexacts, l'utilisation inappropriée des ressources du système, et un surplus de gestion et de soutien pour corriger les problèmes de traitement. | Nous recommandons que le CRSNG limite l'accès « écriture » au répertoire P:/NAMIS/Prod à l'individu responsable de la migration de programmes au système en service, ainsi qu'à son remplaçant autorisé. Cette pratique réduira la possibilité de changements non autorisés au SIGSB. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Moyen | 8. Une vérification du procédé post-octroi a révélé que certaines universités n'avaient soumis aucune documentation au CRSNG pour confirmer l'acceptabilité du bénéficiaire de la subvention.<br>(Se reporter à la page 6.) | Un titulaire d'une subvention inadmissible pourrait continuer de recevoir des paiements. | Nous recommandons un protocole qui oblige les universités à soumettre des pièces justificatives appuyant l'admissibilité des candidats et que ce protocole soit appliqué par l'équipe post-octroi. Si les pièces justificatives ne sont pas fournies, nous recommandons le refus du financement. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | 9. Dans le cas des bourses, une vérification a révélé que les chaires des comités et les agents de programme ne signent pas les chiffriers électroniques de concours. (Ce scénario n'existe pas dans le cas des subventions où la chaire du comité ou l'agent de programme signent physiquement le chiffrier électronique de concours.)<br>(Se reporter à la page 4.) | L'absence d'une approbation officielle rend impossible la vérification de l'approbation des bourses par le comité et leur contrôle par l'agent de programme. | Nous recommandons que le procédé des bourses comprenne la signature officielle de la chaire du comité ainsi que celle de l'agent de programme. Même si le point de démarcation peut changer, selon le nombre de bourses disponibles, cela fournirait une piste de vérification en ce qui a trait au classement établi par le comité. Cela ferait valoir l'obligation de rendre compte. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Moyen | 10. L'accès au système nécessaire pour exécuter les programmes par lots du SIGSB n'est pas contrôlé de façon appropriée. À titre d'exemple, parmi les 13 utilisateurs capables d'exécuter le transfert par lots du financement des subventions à l'étape paiement et les 9 utilisateurs capables d'exécuter le transfert par lots du financement des bourses à l'étape paiement, seulement 2 individus peuvent justifier ce privilège d'accès.<br>(Se reporter à la page 10) | Les privilèges non justifiés pour le traitement par lots dans le SIGSB mettent en jeu l'intégrité de l'information corporative. | Nous recommandons que l'accès nécessaire pour télécharger les chiffriers électroniques de concours et le transfert par lots des fonds de l'étape financement à l'étape paiement dans le SIGSB soit restreint aux individus qui en ont réellement besoin pour effectuer leurs tâches. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | 11. Même s'il existe un procédé par lequel les propriétaires des ressources informationnelles peuvent autoriser l'accès aux utilisateurs, la piste de vérification est inadéquate. À titre d'exemple, les propriétaires des ressources informationnelles ne précisent pas l'accès à « onglets/rapports/utilitaires/programmes », mais spécifient plutôt « accorder lui le même accès que l'utilisateur X ... ». Puisque l'accès accordé à X n'est pas inscrit sur le formulaire, il est impossible de vérifier si les privilèges accordés sont les mêmes que ceux que le propriétaire des ressources informationnelles a approuvé lorsque le formulaire a été rempli.<br><br>Nous avons aussi remarqué que la pertinence de l'accès accordé aux utilisateurs n'est pas examinée régulièrement par les propriétaires des ressources informationnelles.<br><br>De plus, les privilèges d'accès ont été vérifiés pour un groupe de 15 utilisateurs; dans certains cas, il était exagéré. À titre d'exemple, 3 utilisateurs du secteur des finances du groupe possèdaient des privilèges au-delà des exigences de leurs tâches.<br>(Se reporter à la page 10.) | Le procédé utilisé pour accorder les privilèges d'accès est imparfait et l'examen des privilèges d'accès par les propriétaires des ressources informationnelles n'est pas effectué régulièrement. Cela met à risque les actifs de l'organisme et l'intégrité de l'information corporative. | Nous recommandons que les propriétaires des ressources informationnelles du CRSNG autorisent l'accès au niveau de l'onglet, du rapport, de l'utilitaire et du programme. De plus, les propriétaires des ressources informationnelles devraient régulièrement réexaminer les privilèges d'accès.<br><br>Nous recommandons aussi qu'un lien soit établi avec la section des ressources humaines afin de s'assurer que les privilèges d'accès sont mis à jour ou supprimés selon le cas lorsqu'un utilisateur part ou qu'il est muté. |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Moyen | 12. Dans le cas d'essais du SIGSB, les résultats et les procédures d'essai ne sont pas officiellement documentés. Le personnel de l'assurance de la qualité effectue des essais et imprime les résultats, mais il n'existe aucun calendrier pour la rétention des résultats.<br>(Se reporter à la page 14.) | Si les plans d'évaluation et les résultats ne sont pas officiellement documentés et conservés, il risque d'y avoir des problèmes éventuels liés aux changements récemment implémentés dans le SIGSB en raison de la portée trop restreinte des essais.<br>L'approbation officielle des utilisateurs leur transmet un sentiment d'appartenance afin d'assurer l'exécution des essais nécessaires. | Nous recommandons que l'ampleur des essais et les procédures soient documentées avant leur exécution. Une fois les essais préétablis terminés, les utilisateurs devraient apposer leur signature pour officiellement approuver les changements ou les améliorations apportés au système. Cette pratique réduira le risque d'échec dans le dépistage des erreurs au moment de la mise en oeuvre d'un changement au système ou à une application.<br>Finalement, nous recommandons que la documentation d'essai soit conservée afin qu'il existe une piste de vérification en cas de problèmes de traitement éventuels. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Moyen | 13. Même s'il existe un formulaire qui permet aux employés d'apposer leur signature en guise d'approbation de la politique du Conseil sur l'utilisation permise des réseaux électroniques, son utilisation n'a pas été prescrite et la majorité des employés ne l'ont pas signées.<br>(Se reporter à la page 12.) | Il existe un risque considérable que les utilisateurs ne comprennent pas la politique sur l'utilisation permise des réseaux électroniques, ou ne s'y conforment pas. Si les utilisateurs ne sont pas obligés de lire la politique, et de signer le formulaire, il devient difficile pour le CRSNG de l'appliquer. | Nous recommandons que la responsabilité pour la mise en oeuvre de ce procédé soit clairement identifiée et que l'individu responsable effectue le suivi nécessaire afin que le dossier de tous les employés contienne un formulaire signé sur l'utilisation des réseaux électroniques. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Moyen | 14. Nous n'avons trouvé aucun contrat attestant que les conditions ambiantes de l'emplacement d'entreposage des rubans de sauvegarde étaient contrôlées, et aucun membre du personnel du CRSNG n'a visité cet emplacement depuis deux ou trois ans.<br>(Se reporter à la page 13.) | Les causes de dommages aux ressources informationnelles peuvent être nombreuses : chaleur, fumée, feu, humidité, inondation, tremblement de terre et panne électrique. Si les ressources informationnelles ne sont pas adéquatement protégées, elles risquent de ne pas être disponibles quand elles le doivent et, en cas d'urgence, la récupération de ces ressources peut être retardée. | Nous recommandons de modifier le contrat afin de permettre au CRSNG d'effectuer régulièrement une vérification, ou d'obtenir la garantie d'un tiers, des contrôles utilisés à l'emplacement d'entreposage hors site. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Faible | 15. Dans plusieurs cas, la vérification a révélé qu'il était difficile de distinguer les signatures dans les dossiers de concours.<br>(Se reporter à la page 4.) | Les dossiers de concours risquent de ne pas comprendre l'approbation nécessaire, ce qui augmente le risque d'octrois invalides. | Nous recommandons l'utilisation d'un formulaire officiel qui comprend le nom et le titre des signataires autorisés. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Faible | 16. Dans le cas du PPR, les demandes sont traitées par les adjoints des programmes du SIGSB. Les données saisies par SIGSB ne sont pas révisées pour assurer leur exactitude et leur intégralité. Il faut toutefois remarquer qu'aucun point de litige n'est survenu lors de vérification des demandes/fichiers du PPR.<br>(Se reporter à la page 3.) | Il existe un risque que les erreurs de données ne soient pas dépistées puisque aucun mécanisme de surveillance ou d'examen ne suit l'entrée des données. | Nous recommandons la mise en oeuvre d'un procédé, où les agents de programme réviseraient les données entrées dans le SIGSB sur une base empirique afin d'assurer leur exactitude et leur intégrité. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Faible | 17. Les listes de contrôle utilisées pour l'examen des demandes n'accompagnent pas toujours la demande - surtout dans le cas des bourses. Les listes de contrôle ne sont conservées que s'il existe des points en litige qui exigent un suivi.<br>(Se reporter à la page 3.) | Si les listes de contrôle de traitement de demande ne sont pas conservées dans le dossier, il n'existe pas d'éléments probants pour vérifier leur utilisation. De plus, il n'existe aucune piste de vérification si des points en litige surviennent subséquemment. | Nous recommandons que les listes de contrôle de traitement de demande soient conservées dans le dossier de la demande. |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Faible | 18. Plusieurs adjoints des programmes utilisent Excel ou Lotus Notes pour suivre les demandes et comme outil de rappel.<br>(Se reporter à la page 4.) | L'utilisation de systèmes parallèles signifie l'entrée en double des données et augmente le risque d'erreur et d'informations incomplètes. | Nous recommandons au CRSNG d'étudier l'utilisation de systèmes parallèles afin d'établir si cette fonctionnalité pourrait être intégrée au SIGSB.<br><br>Se reporter également à l'Objectif de la vérification 3.4. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |
| Faible | 19. Il n'existe aucun examen des changements apportés aux données de base pour assurer l'exactitude de l'entrée de données, quoique des examens des données à grande échelle soient périodiquement effectués.<br><br>Dans un cas, la vérification a révélé une erreur d'entrée de données au moment de l'inscription d'un nouvel organisme (erreur de frappe dans l'adresse).<br>(Se reporter à la page 5.) | Si l'entrée de données de base du SIGSB n'est pas examinée, le risque d'erreurs et de changements non détectés augmente. | Nous recommandons que les parties intéressées considèrent une révision par un organisme indépendant des changements apportés au fichier maître pour assurer l'intégrité, l'exactitude et la validité des changements apportés au SIGSB. Cette pratique pourrait être facilitée par l'utilisation d'un rapport de changement provenant du SIGSB. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

| Risque | Observation | Conséquences | Recommandation |
|---|---|---|---|
| Faible | 20. Le CRSNG et le CRSH partagent la salle des ordinateurs avec le Conseil des arts du Canada. Le CRSNG n'exerce aucun contrôle sur les membres du personnel du Conseil des arts du Canada qui peuvent accéder à la salle des ordinateurs. (Se reporter à la page 11.) | Les ressources informationnelles du CRSNG comprennent le matériel informatique, les périphériques, des supports de données et la documentation des systèmes informatiques. L'accès physique à de telles ressources permet à l'utilisateur de visionner, d'utiliser, d'endommager ou de détourner ces ressources. | Nous recommandons que l'accès aux ressources informationnelles du CRSNG et du CRSH soit restreint à leurs propres membres du personnel autorisés. |
| Plan d'action du personnel cadre :<br><br>Date d'achèvement prévue :<br>Organisme responsable : | | | |

## *APPENDICE B*

# VUE D'ENSEMBLE DES RÉSULTATS SELON LES CRITÈRES

Voici un résumé des exigences qui indique si le système répond aux exigences (√), répond partiellement aux exigences (–) ou s'il ne répond pas aux exigences *(X)*.

| **Objectif de la vérification** | **Critère de vérification** | **Référence (page)** | **Résultat** | | |
|---|---|---|---|---|---|
| **Section 3 - Contrôles des processus opérationnels** | | | | | |
| 3.1 S'assurer que le SIGSB respecte les règles administratives améliorées nécessaires visant :<br>• à garantir l'intégrité des données,<br>• à gérer et à suivre les demandes durant le cycle de vie de l'octroi de subventions du CRSNG,<br>• à accepter et à enregistrer la demande initiale,<br>• à observer la sélection par les pairs,<br>• à gérer les subventions post-octrois,<br>• à communiquer des données. | 1.1 | 3 | √ | | |
| | 1.2 | 4 | | – | |
| | 1.3 | 4 | √ | | |
| | 1.4 | 5 | | | *X* |
| | 1.5 | 5 | *Se reporter à la section 4* | | |
| 3.2 S'assurer que le SIGSB comprend les contrôles nécessaires pour le suivi du financement et des paiements. | 2.1 | 6 | √ | | |
| | 2.2 | 6 | | – | |
| | 2.3 | 6 | √ | | |
| | 2.4 | 7 | | | *X* |
| | 2.5 | 7 | *Se reporter à la section 4* | | |

| **Objectif de la vérification** | **Critère de vérification** | **Référence (page)** | **Résultat** | | |
|---|---|---|---|---|---|
| 3.3 S'assurer que le système possède les contrôles nécessaires pour toute information financière du SIGSB transmise au SFAGAI. | 3.1 | 7 | √ | | |
| | 3.2 | 8 | *Se reporter à la section 4* | | |
| **Section 4 - Contrôles informatiques généraux** | | | | | |
| 4.1 Les traitements par lots sont effectués selon les délais prescrits et de façon intégrale. | 1.1 | 9 | √ | | |
| 4.2 Seuls les programmes en service valides sont exécutés. | 2.1 | 9 | | | X |
| 4.3 Toutes les données financières sont transférées du SIGSB au SFAGAI (interface). | 3.1 | 10 | √ | | |
| 4.4 Des outils et des techniques de sécurité logique sont élaborés et configurés afin de restreindre l'accès au SIGSB. | 4.1 | 10 | √ | | |
| 4.5 Les outils et des techniques de sécurité logique sont gérés de façon à restreindre l'accès aux programmes, aux données et à certaines autres ressources informationnelles du SIGSB. | 5.1 | 10 | | | X |
| 4.6 Des contrôles d'accès physique sont mis en oeuvre et gérés afin de s'assurer que seulement les individus autorisés peuvent accéder aux ressources informationnelles ou les utiliser. | 6,1 | 11 | √ | | |
| 4.7 Les ressources informationnelles sont protégées contre les risques environnementaux et les dommages connexes. | 7.1 | 12 | √ | | |
| 4.8 Les politiques et les procédures pour l'administration complète et la mise en oeuvre de la sécurité informatique sont documentées. | 8.1 | 12 | √ | | |

| **Objectif de la vérification** | **Critère de vérification** | **Référence (page)** | **Résultat** | | |
|---|---|---|---|---|---|
| | 8.2 | 12 | | | X |
| 4.9 En cas de désastre, les systèmes informatiques et les processus opérationnels essentiels peuvent être récupérés en peu de temps. | 9.1 | 13 | √ | | |
| | 9.2 | 13 | √ | | |
| | 9.3 | 13 | √ | | |
| | 9.4 | 13 | *Aucune conclusion* | | |
| | 9.5 | 13 | √ | | |
| 4.10 La mise en oeuvre du SIGSB est effectuée de façon adéquate et celui-ci fonctionne conformément aux attentes du personnel cadre, et toutes les modifications nécessaires du SIGSB sont effectuées selon les délais prescrits. | 10.1 | 14 | | | X |
| | 10.2 | 14 | | | X |
| 4.11 Les logiciels de réseau et de communication sont mis en oeuvre de façon appropriée et fonctionnent selon les intentions du personnel cadre et les modifications intégrées à ces logiciels sont effectuées selon les délais prescrits. | 11.1 | 15 | | | X |
| | 11.2 | 15 | | | X |
| 4.12 Les logiciels de base sont mis en oeuvre de façon appropriée et fonctionnent selon les intentions du personnel cadre et les modifications intégrées à ces logiciels sont effectuées selon les délais prescrits. | 12.1 | 16 | | | X |
| | 12.2 | 16 | | | X |

| Objectif de la vérification | Critère de vérification | Référence (page) | Résultat | | |
|---|---|---|---|---|---|
| 4.13 Les stratégies, les plans et les budgets des systèmes informatiques sont compatibles avec les objectifs et la stratégie de l'organisme. | 13.1 | 17 | √ | | |
| 4.14 Le niveau de service offert par les fournisseurs d'impartition répond aux attentes du personnel cadre, ou les dépasse. | 14.1 | 17 | *Sans objet* | | |

## *APPENDICE C*

# VUE D'ENSEMBLE DE LA CONVIVIALITÉ ET DE L'AMPLEUR DE LA PORTÉE

Le graphique ci-dessous offre une vue d'ensemble des réponses des groupes de discussion portant sur chacune des questions suivantes : fonctionnalité, aide et soutien, architecture de système et expérience de l'utilisateur.

**1 Très satisfait**
**2 Satisfait (quelques améliorations souhaitables)**
**3 Insatisfait (plusieurs améliorations nécessaires)**
**4 Très insatisfait (améliorations obligatoires)**