

Considérations pour l'évaluation du risque de contrôle lié à l'activité d'un site (Partie 3)

Dans les précédents dossiers, nous avons stratifié l'évaluation du système de contrôle interne lié à l'activité d'un site Web en étudiant, d'abord l'environnement de contrôle, puis les contrôles généraux du système informatique et les sécurités du serveur et applications Web. Dans cette troisième et dernière partie, nous allons achever notre exploration du système de contrôle interne lié à l'activité du site en analysant les contrôles spécifiques, soutenant certains principes généralement admis, qui doivent encadrer les transactions et les opérations d'un site Web. Ces principes sont largement inspirés de ceux publiés par l'AICPA¹ et le CICA² dans leur programme WebTrust destiné à la certification des sites de commerce électronique. Ce programme énonce des principes et des critères types découlant d'un consensus de bonnes pratiques ô combien nécessaires pour régir les transactions et les opérations sur un site de e-commerce. Au nombre de cinq, ces principes s'énoncent comme suit :

- 1- protection des renseignements personnels en ligne,
- 2- transparence des pratiques commerciales et intégrité des opérations,
- 3- sécurité des données,
- 4- confidentialité des données,
- 5- accessibilité su site.

Il est à noter, au passage, que chaque principe constitue une attente cruciale de chaque internaute et de chaque intervenant dans une transaction de e-commerce. Pour qu'ils soient validés, chaque principe est assorti d'une suite de critères touchant aux informations à fournir sur le site, à la politique de l'entité, aux procédures de contrôle interne proprement dites et au système de surveillance mis en place. Ainsi, un principe n'est validé que si l'ensemble de ses critères inhérents sont eux aussi respectés. Dans cette étape spécifique, l'évaluation du système de contrôle interne s'attarde donc à analyser l'existence, la conformité et l'application des contrôles mis en place pour respecter ces critères et leur principe fondateur.

Comme pour les précédentes étapes, nous allons proposer des outils de travail pour l'expert comptable pour parachever son évaluation du système de contrôle interne, dans cette dernière « strate » touchant aux transactions du site. Nous rappelons, à ce propos, que ces questionnaires ne constituent qu'une indication de travail et ne peuvent être considérées comme une référence absolue, ou se substituer aux diligences et au bon sens que l'expert comptable doit déployer.

4. Check-list pour le principe de transparence des pratiques commerciales et d'intégrité des opérations :

<i>Check-list pour l'évaluation du contrôle interne pour le principe de transparence des pratiques commerciales et d'intégrité des opérations</i>	O	N	N/A	WP REF
> Informations				
1. L'entité fournit-elle une information descriptive sur la nature des biens qui seront livrés ou des services qui seront fournis en mentionnant notamment :				

¹ American Institute of Certified Public Accountants

² Canadian Institute of Chartered Accountants

<p>a. l'état des biens (s'ils sont neufs, d'occasion ou remis à neuf);</p> <p>b. la description des services (ou du contrat de service);</p> <p>c. les sources des informations (comment elles ont été obtenues et comment elles sont établies) ?</p> <p>2. L'entité décrit-elle les modalités de ses opérations de commerce électronique en indiquant notamment :</p> <p>a. le délai d'exécution des opérations (le terme «opération» se rapporte à l'exécution des commandes dans le cas de la vente de biens et à la prestation d'un service dans le cas où un service est fourni);</p> <p>b. le délai et le mode de notification du client en cas de dérogations au traitement habituel des commandes ou des demandes de services;</p> <p>c. le mode habituel de livraison des biens ou de prestation des services, y compris les options offertes au client, le cas échéant;</p> <p>d. les modalités de paiement, y compris les options offertes au client,</p>				
<p>e. les modalités de règlement électronique et les frais connexes facturés au client;</p> <p>f. la façon dont le client peut mettre fin à ses frais périodiques, le cas échéant;</p> <p>g. la politique concernant les retours sur achats de produits et la limitation de responsabilité, le cas échéant ?</p> <p>3. L'entité indique-t-elle (sur son site Web ou dans les documents fournis avec le produit) où les clients peuvent faire valoir leur garantie et obtenir un service de réparation et un soutien après-vente pour les biens et services achetés par le truchement de son site Web ?</p> <p>4. L'entité donne-t-elle aux clients les informations qui leur permettent de déposer des réclamations, de poser des questions ou de formuler des plaintes, notamment :</p> <p>a. le numéro de téléphone (un numéro où il possible de joindre un employé dans un délai raisonnable et non pas un système de boîte vocale ou un répondeur);</p> <p>b. les jours et les heures d'ouverture?</p> <p>c. Si l'entité possède plusieurs bureaux ou succursales, les informations ci-dessus doivent également être fournies pour le siège social.</p> <p>5. L'entité indique-t-elle le processus suivi pour permettre au client d'exercer un recours en cas de différend concernant l'intégrité des opérations que l'entité ne peut résoudre? Les différends peuvent toucher n'importe quel aspect de l'opération de commerce électronique effectuée par le client, y compris les plaintes relatives à la qualité des produits et des services, à l'exactitude, à l'exhaustivité, ainsi que les conséquences découlant de l'incapacité de régler ces plaintes. Ce processus de résolution devrait comporter les caractéristiques suivantes :</p> <p>a. l'engagement de la direction à faire appel à un service de règlement de différends dispensé par un tiers désigné à cette fin, s'il s'avère que le client n'est pas satisfait du règlement proposé par l'entité à l'égard de la plainte;</p> <p>b. les procédures à suivre pour régler les plaintes, d'abord auprès de l'entité puis, si nécessaire, auprès du tiers désigné.</p> <p>6. L'entité indique-t-elle aux particuliers, aux entreprises et aux autres utilisateurs comment ils peuvent l'informer au sujet des brèches réelles ou présumées en ce qui concerne l'intégrité (y compris la sécurité) de son ou ses systèmes de commerce électronique ?</p> <p>7. L'entité indique-t-elle la nature des services d'applications courants qui sont offerts aux clients d'affaires et la mesure dans laquelle ses pratiques commerciales déclarées et ses contrôles sur l'intégrité des opérations s'appliquent à ces services ?</p>				
<p>> Politiques</p> <p>1. Les politiques de l'entité en matière d'intégrité des opérations comprennent-elles les éléments suivants au minimum :</p> <p>a. qui a l'autorisation d'accès, quelle est la nature de cet accès et qui accorde cette autorisation;</p> <p>b. procédures pour ajouter de nouveaux utilisateurs, modifier les niveaux d'accès des utilisateurs actuels et retirer l'accès aux utilisateurs qui n'en ont plus besoin;</p>				

<p>c. procédures de sécurité visant la protection de l'intégrité des opérations; d. procédures permettant de documenter les opérations et d'en faire le suivi; e. façon dont les plaintes et les demandes relatives aux opérations peuvent être traitées; f. procédures pour traiter les atteintes à la sécurité; g. engagement de l'entité à utiliser un service de règlement de différends offert par un tiers qui soit conforme aux principes d'arbitrage internationaux ?</p> <p>2. De quelle façon les employés responsables de l'intégrité des opérations connaissent-ils et respectent-ils les politiques déclarées de l'entité relatives à l'intégrité des opérations et aux questions de sécurité pertinentes ?</p> <p>3. Indiquez qui est responsable des politiques de l'entité relatives à l'intégrité des opérations et aux questions de sécurité pertinentes.</p>				
<p>4. Les politiques de l'entité relatives à l'intégrité des opérations et aux questions de sécurité pertinentes concordent-elles avec ses pratiques commerciales déclarées et les lois et règlements en vigueur ?</p>				
<p>> <u>Procédures</u></p> <p><i>Pour les critères de sécurité liés à l'intégrité des opérations :</i></p> <p>1. L'entité a-t-elle établi des procédures visant les nouveaux utilisateurs? 2. L'entité a-t-elle établi des procédures permettant d'identifier et d'authentifier les utilisateurs autorisés ? 3. L'entité a-t-elle établi des procédures permettant aux utilisateurs de modifier, de mettre à jour et de supprimer leur propre profil ? 4. L'entité a-t-elle établi des procédures grâce auxquelles l'accès à distance au réseau interne est réservé aux employés autorisés ? 5. L'entité a-t-elle établi des procédures visant à empêcher des clients, des groupes de personnes ou d'autres entités d'accéder à des informations sur les opérations autres que les leurs? 6. L'entité a-t-elle établi des procédures visant à restreindre l'accès aux systèmes et aux données aux seuls employés autorisés, selon les rôles et les responsabilités qui leur sont confiés ? 7. L'entité applique-t-elle le chiffrement ou d'autres mesures de sécurité équivalentes pour éviter que l'information sur l'authentification et la vérification des utilisateurs soit interceptée sur Internet ? 8. L'entité a-t-elle établi des procédures visant à maintenir des configurations de système qui minimisent les risques pour l'intégrité des opérations et la sécurité ? 9. L'entité a-t-elle établi des procédures pour surveiller les brèches de sécurité qui touchent l'intégrité des opérations et pour agir en conséquence ?</p> <p><i>Demandes de biens et de services :</i></p> <p>10. L'entité vérifie-t-elle l'exactitude et l'exhaustivité de chaque demande ou opération ? 11. L'entité obtient-elle une confirmation du client avant le traitement de l'opération ?</p> <p><i>Traitement des demandes de biens et de services :</i></p> <p>12. Les bons articles sont-ils livrés conformément aux quantités et aux délais convenus, ou les informations et les services sont-ils fournis au client comme demandé ? 13. Les anomalies relatives aux opérations sont-elles communiquées sans délai au client ? 14. Les messages d'arrivée sont-ils traités et transmis correctement et intégralement à la bonne adresse IP ? 15. Les messages de départ sont-ils traités et transmis correctement et intégralement au point d'accès Internet du fournisseur de services (FS)? 16. Les messages restent-ils intacts lorsqu'ils circulent dans les limites du réseau du FS ?</p>				

<p><i>Traitement, factures et paiements :</i></p> <p>17. Les prix de vente et tous les autres coûts/frais sont-ils affichés à l'intention du client avant que le traitement de l'opération ne commence ?</p> <p>18. Les opérations sont-elles facturées et réglées par voie électronique comme convenu ?</p> <p>19. Les erreurs de facturation ou de règlement sont-elles corrigées rapidement ?</p> <p>20. Conserve-t-on l'historique des opérations dans un endroit sûr où il ne peut être modifié sans autorisation appropriée ? L'information peut-elle être consultée aux fins d'examen et d'enquête ?</p>				
<p>21. Les opérations sont-elles traitées correctement et en conformité avec les pratiques commerciales déclarées de l'entité ?</p> <p>22. L'entité consigne-t-elle les opérations afin d'effectuer un suivi ultérieur ?</p>				
<p>> Surveillance</p> <p>1. L'entité a-t-elle établi des procédures afin de surveiller les opérations de ses systèmes de commerce électronique et de repérer les changements nécessaires à ses politiques d'intégrité des opérations et aux contrôles de sécurité connexes ?</p> <p>2. L'entité a-t-elle mis en place des procédures afin que l'historique des opérations et l'information connexe soient surveillées et que des mesures correctrices soient prises régulièrement et rapidement ?</p>				

5. Check-list pour le principe de protection des renseignements personnels :

Check-list pour l'évaluation du contrôle interne pour le principe de protection des renseignements à caractère personnel	O	N	N/A	WP REF
<p>> Informations</p> <p>1. L'entité décrit-elle pratiques de protection des renseignements personnels et les pratiques de sécurité connexes de l'entité et la façon dont les clients en sont informés, telles que :</p> <p>a. Types et sources des renseignements recueillis, par exemple :</p> <ul style="list-style-type: none"> i) nom, ii) adresse, iii) type d'ordinateur, iv) numéro de carte de crédit, v) adresse électronique, vi) autres renseignements pertinents. <p>b. Utilisation des renseignements recueillis :</p> <ul style="list-style-type: none"> i) envoi d'informations sur la société, ii) facturation des produits commandés par les clients, iii) envoi de documents publicitaires provenant de partenaires ou à leur sujet, iv) autres utilisations des renseignements personnels, s'il y a lieu. <p>c. Possibilité que les renseignements recueillis soient communiqués à des tiers.</p> <p>d. Possibilité de mentionner toute limite quant à la mesure dans laquelle l'entité se fie aux pratiques et contrôles de ces tiers en matière de protection des renseignements personnels. Ces tiers peuvent être notamment :</p> <ul style="list-style-type: none"> i) des parties qui interviennent dans l'opération (par exemple, entreprise de traitement de cartes de crédit, services de livraison et d'exécution des commandes), ii) des parties n'ayant pas de lien avec l'opération (par exemple, entreprises de marketing auxquelles l'information est transmise). <p>e. Choix relatifs à la façon dont des renseignements personnels recueillis électroniquement auprès du client peuvent être utilisés ou diffusés :</p> <ul style="list-style-type: none"> i) possibilité de refuser de les fournir, ii) possibilité de refuser leur communication à des tiers qui ne sont pas 				

<p>parties à l'opération, iii) autres.</p> <p>f. Façon dont les personnes donnent leur consentement avant que les renseignements personnels nécessaires à l'opération de commerce électronique soient recueillis et transmis.</p> <p>g. Conséquences, s'il en est, du refus d'une personne de fournir des renseignements ou de la décision de ne pas donner son consentement à une utilisation particulière de ces renseignements.</p>				
<p>h. Façon dont les renseignements personnels erronés ou incomplets peuvent être examinés par le client et, au besoin, corrigés ou supprimés ?</p> <p>2. Si le site Web utilise des témoins (cookies) ou d'autres méthodes de suivi (par exemple des parasites du Web, spyware, adware...), l'entité indique-t-elle de quelle façon ceux-ci sont utilisés et quelles sont les conséquences, s'il en est, du refus d'une personne d'accepter un témoin ?</p> <p>3. L'entité décrit-elle l'information communiquée par l'entité aux particuliers, aux entreprises et aux autres utilisateurs pour permettre à ceux-ci de l'informer au sujet de brèches réelles ou possibles à la protection des renseignements personnels et à la sécurité de son ou ses systèmes de commerce électronique ?</p> <p>4. L'entité indique-t-elle aux clients les canaux permettant de poser des questions ou d'obtenir de l'aide ?</p> <p>5. L'entité décrit-elle les procédures mises en place par l'entité pour résoudre les différends, y compris au minimum les suivantes :</p> <ul style="list-style-type: none"> a. Procédures à suivre pour régler les plaintes, d'abord avec l'entité. b. Résolution des plaintes relatives à l'exactitude, à l'intégralité et à la diffusion des renseignements personnels. c. Utilisation qui sera faite des renseignements personnels faisant l'objet de la plainte ou mesures qui seront prises à leur égard, jusqu'au règlement satisfaisant de la plainte. d. Coordonnées de la personne-ressource pour tout organisme gouvernemental qui reçoit les plaintes des consommateurs sur les questions de protection des renseignements personnels. e. Engagement de la direction à recourir à un service de règlement des différends offert par un tiers désigné à cette fin, s'il s'avère que le client n'est pas entièrement satisfait du règlement proposé par l'entité à l'égard de la plainte. f. Engagement de ce tiers à régler les plaintes non réglées ? <p>6. L'entité indique-t-elle le processus utilisé pour définir et communiquer les modifications ou mises à jour de ses pratiques de protection des renseignements personnels et de ses pratiques de sécurité connexes afin de se conformer aux lois et règlements en vigueur ou à tout programme d'auto-réglementation auquel elle participe ?</p> <p>7. L'entité indique-t-elle aux visiteurs qu'ils ont quitté la partie du site couverte par sa politique de protection des renseignements personnels au moment opportun ?</p>				
<p><u>> Politiques, buts et objectifs</u></p> <p>1. L'entité a-t-elle une politique en matière de protection des renseignements personnels, notamment les éléments suivants :</p> <ul style="list-style-type: none"> a. Avis au client quant aux renseignements recueillis. b. Choix du client quant au(x) type(s) de renseignements recueillis et toute option offerte au client à cet égard. c. Procédures pour ajouter de nouveaux utilisateurs, modifier les niveaux d'accès des utilisateurs actuels et retirer l'accès aux utilisateurs qui n'en ont plus besoin. d. Détermination des employés ayant un accès autorisé en raison de leurs responsabilités et de la personne qui autorise cet accès. e. Accès du client à ses renseignements personnels en vue de les mettre à jour ou de les corriger. f. Façon dont les plaintes relatives à la protection des renseignements personnels peuvent être traitées. g. Procédures pour traiter les atteintes à la sécurité. 				

<p>h. Pratiques de conservation et de destruction des dossiers.</p> <p>i. Engagement de l'entité à utiliser un service de règlement de différends offert par un tiers ?</p> <p>2. Existe-t-il des procédures permettant aux responsables de la protection des renseignements personnels d'être mis au courant de la politique publiée par l'entité en matière de protection des renseignements personnels et les politiques de sécurité</p>				
<p>connexes, et quelles mesures sont prises pour voir à ce que les employés respectent ces politiques ?</p> <p>3. Les responsabilités de la politique en matière de protection des renseignements personnels et des politiques de sécurité connexes ont-elles été clairement confiées ?</p> <p>4. Existe-t-il des procédures de formation et des ressources visant à appuyer la politique en matière de protection des renseignements personnels et les politiques de sécurité connexes ?</p> <p>5. Y a-t-il des procédures employées pour évaluer si la politique en matière de protection des renseignements personnels et les politiques de sécurité connexes de l'entité correspondent à ses pratiques déclarées et aux lois et règlements en vigueur ?</p>				
<p><u>> Procédures et outils technologiques</u></p> <p><i>Critères de sécurité liés à la protection des renseignements personnels :</i></p> <p>1. Les critères de sécurité de l'entité liés à la protection des renseignements personnels sont-ils respectés, notamment :</p> <ul style="list-style-type: none"> a. Procédures de sécurité visant les nouveaux utilisateurs. b. Procédures permettant d'identifier et d'authentifier les utilisateurs autorisés. c. Procédures permettant aux utilisateurs de modifier, de mettre à jour et de supprimer leur propre profil. d. Procédures permettant de réserver aux employés autorisés l'accès à distance au réseau. e. Procédures de nature à empêcher des clients, des groupes de personnes ou d'autres entités d'accéder à des renseignements personnels ou sensibles autres que les leurs. f. Procédures visant à restreindre l'accès aux renseignements personnels aux seuls employés autorisés, selon les rôles et les responsabilités qui leur sont confiés. g. Utilisation du chiffrement à 128 bits au minimum pour éviter que l'authentification, la vérification et les renseignements personnels ou sensibles soient interceptés par des destinataires non souhaités lors de leur transmission sur Internet. h. Procédures visant à maintenir des configurations de système qui minimisent les risques susceptibles de compromettre la sécurité des renseignements personnels ou sensibles. <p><i>Critères propres à la protection des renseignements personnels :</i></p> <p>2. Existe-t-il des contrôles et procédures visant à :</p> <ul style="list-style-type: none"> a. Assurer que les renseignements personnels du client obtenus dans le cadre d'une opération de commerce électronique ne sont communiqués qu'aux tiers qui jouent un rôle essentiel dans l'opération, à moins que le client n'en ait été clairement informé avant de fournir ces renseignements. Dans le cas contraire, la permission du client est obtenue avant que les renseignements ne soient divulgués à des tiers. b. Prendre des mesures pour que les renseignements personnels obtenus dans le cadre d'une opération de commerce électronique ne soient utilisés par les employés que pour les besoins des activités de l'entité. c. Prendre des mesures pour que les renseignements personnels recueillis, créés ou conservés soient soumis à des contrôles de validation raisonnables. d. Déterminer l'adéquation des politiques de protection des renseignements personnels adoptées par les tiers à qui les renseignements sont transmis et sur lesquelles l'entité s'appuie, et leur conformité avec ses pratiques déclarées en 				

<p>matière de protection des renseignements personnels.</p> <p>e. Prendre des mesures pour que la permission du client soit obtenue avant de télécharger des données pour les stocker, les modifier ou les copier dans l'ordinateur du client ou pour informer le client qu'il a le choix d'empêcher ces activités :</p> <p>i) s'assurer que des témoins ne sont pas stockés dans l'ordinateur du client si le client a indiqué qu'il n'en veut pas;</p> <p>ii) s'assurer d'avoir obtenu la permission du client avant de stocker, de modifier ou de copier des données (autres que des témoins) dans l'ordinateur du client.</p> <p>Protéger les renseignements personnels conformément aux politiques déclarées en vigueur lorsque ces renseignements ont été recueillis dans le cadre d'une modification ou d'une suppression partielle des politiques en vue de les rendre moins restrictives. Pour que l'entité applique la nouvelle politique à l'égard des renseignements personnels d'un client, ce dernier doit en avoir été informé clairement auparavant et avoir donné son consentement explicite.</p>				
<p>> Surveillance et mesures de la performance</p> <p>1. Existe-t-il des procédures de surveillance relatives à la sécurité des systèmes de commerce électronique ?</p> <p>2. Les procédures en place pour que la politique déclarée de protection des renseignements personnels et les politiques de sécurité connexes sont-elles conformes aux lois et règlements et veillent-elles à ce que les pratiques en vigueur soient respectées ?</p> <p>3. Existe-il des procédures en place pour tester la politique en matière d'atteinte à la sécurité et la mettre à jour au besoin pour tenir compte de l'évolution technologique, des modifications apportées à la structure des systèmes de commerce électronique ou de l'information tirée de ces tests ?</p> <p>4. Les procédures en place pour surveillent-elles efficacement les brèches à la protection des renseignements personnels et à la sécurité, et permettent-elles de prendre les mesures qui s'imposent ?</p>				

6. Check-list pour le principe de sécurité des données :

<i>Check-list pour l'évaluation du contrôle interne pour le principe de sécurité des données</i>	O	N	N/A	WP REF
<p>> Informations</p> <p>1. L'entité indique-t-elle ses pratiques de sécurité relatives à l'accès à son système et aux données de commerce électronique, notamment sur les aspects suivants :</p> <p>a. enregistrement et autorisation des nouveaux utilisateurs;</p> <p>b. identification et authentification des utilisateurs autorisés;</p> <p>c. maintien et suppression de l'accès pour les utilisateurs autorisés ?</p> <p>2. L'entité indique-t-elle aux particuliers, aux entreprises et aux autres utilisateurs comment ils peuvent l'informer au sujet de brèches réelles ou présumées en ce qui concerne la sécurité de son/ses système(s) de commerce électronique ?</p> <p>3. L'entité indique-t-elle les procédures de recours dont disposent les clients à l'égard des problèmes liés à la sécurité ? Ce processus de règlement devrait comporter les caractéristiques suivantes :</p> <p>a. engagement de la direction à recourir à un service de règlement de différends offert par un tiers désigné à cette fin, ou à d'autres processus imposés par des organismes de réglementation, s'il s'avère que le client n'est pas satisfait du règlement proposé par l'entité à l'égard de la plainte, et engagement du tiers à traiter les plaintes non réglées;</p> <p>b. procédures à suivre pour régler les plaintes, d'abord avec l'entité, puis, s'il y a lieu, avec le tiers désigné.</p> <p>4. L'entité indique-t-elle ses applications courantes, le matériel, les logiciels et les diverses fonctions qu'elle offre à d'autres personnes, utilisateurs ou groupes, et indique-t-elle dans quelle mesure ses informations sur la sécurité et ses contrôles portent sur ces fonctions ?</p>				

<p>> Politiques</p> <ol style="list-style-type: none"> 1. les politiques de l'entité en matière de sécurité s'appliquent-elles au système de commerce électronique et comprennent-elles notamment les éléments suivants : <ol style="list-style-type: none"> a. qui a l'autorisation d'accès, quelle est la nature de cet accès et qui accorde cette autorisation; b. procédures pour ajouter de nouveaux utilisateurs, modifier les niveaux d'accès des utilisateurs actuels et retirer l'accès aux utilisateurs qui n'en ont plus besoin; c. personnes responsables de la sécurité, des mises à niveau du système, des sauvegardes et de la maintenance; d. type de scripts ou programmation autorisés sur les pages; e. procédure pour tester et évaluer le logiciel, les pages et les scripts avant de les installer; f. contrôles exercés sur l'accès physique au système; g. façon de résoudre les plaintes et de répondre aux demandes portant sur le contenu du serveur et des pages; h. procédures pour traiter les atteintes à la sécurité; i. engagement de l'entité à utiliser un service de règlement de différends offert par un tiers qui soit conforme aux principes d'arbitrage internationaux ? 2. Comment les employés responsables de la sécurité connaissent-ils et respectent-ils les politiques de l'entité en matière de sécurité ? 3. Qui est responsable des politiques de l'entité en matière de sécurité ? 4. L'entité a-t-elle prévu un programme de formation et d'autres ressources pour ses politiques en matière de sécurité ? 5. Les politiques de sécurité de l'entité correspondent-elles à ses pratiques indiquées et aux lois et règlements en vigueur ? 				
<p>> Procédures</p> <ol style="list-style-type: none"> 1. L'entité a-t-elle établi des procédures de sécurité visant les nouveaux utilisateurs ? 2. L'entité a-t-elle établi des procédures permettant d'identifier et d'authentifier les utilisateurs autorisés ? 3. L'entité a-t-elle établi des procédures permettant aux utilisateurs de modifier, de mettre à jour et de supprimer leur propre profil? 4. L'entité a-t-elle établi des procédures visant à limiter l'accès à distance au réseau interne au personnel autorisé ? <ol style="list-style-type: none"> a. L'entité a-t-elle établi des procédures visant à protéger les systèmes internes contre les virus et les programmes malveillants? b. L'entité a-t-elle établi des procédures visant à empêcher l'accès commuté et non sécurisé à Internet en cours de session sur le réseau local ? c. L'entité a-t-elle établi des procédures visant à réduire ou à éliminer les services réseau inutiles (numéros de port) ? d. L'entité a-t-elle établi des procédures visant à mettre à niveau ses logiciels à la version optimale et à apporter des correctifs au besoin ? 5. L'entité a-t-elle établi des procédures visant à empêcher des clients, des groupes de personnes ou d'autres entités d'accéder à des renseignements personnels ou sensibles autres que les leurs ? 6. L'entité a-t-elle établi des procédures visant à limiter l'accès aux systèmes et aux données aux seuls employés autorisés, en fonction des rôles et des responsabilités qui leur sont confiés ? <ol style="list-style-type: none"> a. L'entité a-t-elle établi des procédures pour protéger les mots de passe principaux ou de «super-utilisateur» et ne permet-elle qu'à un petit nombre d'employés autorisés d'accéder à ces mots de passe ? b. L'entité a-t-elle établi des procédures pour empêcher les employés non autorisés d'accéder aux postes de travail inactifs ? c. L'entité limite-t-elle l'accès physique aux pare-feu, aux serveurs et à d'autres systèmes critiques aux seuls employés autorisés ? d. L'entité protège-t-elle ses programmes et ses données pendant les processus de sauvegarde, de stockage hors lieux et de restauration ? 7. L'entité utilise-t-elle le chiffrement ou d'autres mesures de sécurité équivalentes pour éviter que les renseignements concernant l'authentification et la vérification des 				

<p>utilisateurs soient interceptés lors de leur transmission sur Internet ?</p> <p>8. L'entité a-t-elle établi des procédures visant à maintenir des configurations de système qui minimisent les risques pour la sécurité ?</p> <p>9. L'entité a-t-elle établi des procédures pour surveiller les brèches en ce qui concerne la sécurité et pour agir en conséquence ?</p> <p>10. L'entité a-t-elle défini des normes de programmation – et s'y conforme-t-elle – et effectue-t-elle des tests de logiciels dans un environnement contrôlé pour s'assurer que les pages Web utilisant des technologies de contenu actif (par exemple, applets Java, ActiveX et JavaScript) ne sont pas exposées à des faiblesses sur le plan de la sécurité ?</p>				
<p><u>> Surveillance</u></p> <p>1. L'entité a-t-elle établi des procédures pour surveiller la sécurité de ses systèmes de commerce électronique et pour relever les modifications à apporter à ses procédures de sécurité ?</p> <p>2. L'entité a-t-elle établi des procédures pour surveiller sa politique en matière d'atteinte à la sécurité et la mettre à jour au besoin pour tenir compte de l'évolution technologique, des modifications apportées à la structure des systèmes de commerce électronique, ou d'autres informations ?</p> <p>3. L'entité a-t-elle établi des procédures pour surveiller les changements environnementaux et technologiques ainsi que les risques connexes et leur incidence sur ses pratiques de sécurité ?</p> <p>4. L'entité a-t-elle établi des procédures pour s'assurer que les rapports de non-conformité aux informations et aux contrôles relatifs à la sécurité sont pris en considération et que des correctifs sont apportés régulièrement et rapidement ?</p>				

7. Check-list pour le principe d'accessibilité :

<i>Check-list pour l'évaluation du contrôle interne pour le principe d'accessibilité</i>	O	N	N/A	WP REF
<p><u>> Informations</u></p> <p>1. L'entité indique-t-elle les modalités et pratiques concernant l'accessibilité de son centre informatique, de son réseau et du réseau fédérateur Internet ?</p> <p>2. L'entité indique-t-elle les procédures que les particuliers, les sociétés ou d'autres utilisateurs peuvent suivre pour l'informer des brèches réelles ou présumées en ce qui concerne la sécurité de son/ses système(s) de commerce électronique ?</p> <p>3. L'entité indique-t-elle les voies de recours dont dispose le client pour les problèmes d'accessibilité des systèmes non résolus par l'entité ? Ce processus de résolution devrait comporter les caractéristiques suivantes :</p> <p>a. l'engagement de la direction à faire appel à un service de règlement de différends dispensé par un tiers désigné à cette fin, ou à d'autres processus imposés par des organismes de réglementation, s'il s'avère que le client n'est pas satisfait du règlement proposé par l'entité à l'égard de la plainte, et l'engagement de ce tiers à traiter les plaintes non réglées;</p> <p>b. les procédures à suivre pour régler les plaintes, d'abord auprès de l'entité puis, si nécessaire, auprès du tiers désigné.</p> <p>4. L'entité indique-t-elle les applications courantes, le matériel, le logiciel et les diverses fonctions qu'elle offre à d'autres personnes, utilisateurs ou groupes, et la mesure dans laquelle ses informations et ses contrôles portent sur l'accessibilité de ces fonctions ?</p>				
<p><u>> Politiques</u></p> <p>1. Les politiques de l'entité sur l'accessibilité du système et des données de commerce électronique portent-elles notamment sur les aspects suivants :</p> <p>a. les personnes qui ont accès au système, la nature de l'accès et la personne qui autorise l'accès;</p> <p>b. les procédures pour l'ajout de nouveaux utilisateurs, la modification des niveaux d'accès des utilisateurs actuels et le retrait de l'accès aux utilisateurs qui n'en ont plus besoin;</p> <p>c. la personne responsable de la sécurité, des mises à niveau, de la sauvegarde et de la maintenance du système;</p>				

<p>d. les plans antisinistres et les plans de poursuite des activités;</p> <p>e. les contrôles relatifs à l'accès physique;</p> <p>f. la façon dont les plaintes relatives à l'accessibilité peuvent être traitées;</p> <p>g. les procédures visant le traitement des brèches de sécurité;</p> <p>h. le processus de surveillance de l'accessibilité du système indiquée;</p> <p>i. l'engagement de l'entité à confier à un tiers le règlement de différends en conformité avec les principes d'arbitrage internationaux.</p> <p>2. Comment les employés responsables de l'accessibilité sont-ils informés des politiques de l'entité concernant l'accessibilité et des questions de sécurité pertinentes et quelles obligations ont-ils à cet égard ?</p> <p>3. Indiquez le nom de la personne responsable des politiques de l'entité en matière d'accessibilité et des questions de sécurité pertinentes.</p> <p>4. L'entité a-t-elle prévu un programme de formation et d'autres ressources pour ses politiques d'accessibilité et les questions de sécurité pertinentes ?</p> <p>5. Les politiques de l'entité concernant l'accessibilité et les questions de sécurité pertinentes correspondent-elles à ses exigences déclarées, aux pratiques en matière de sécurité et aux lois et règlements applicables ?</p>				
<p>> <u>Procédures</u></p> <p><i>Eléments de la sécurité concernant l'accessibilité</i></p> <p>1. L'entité a-t-elle mis en place des procédures en matière de sécurité pour les nouveaux utilisateurs ?</p> <p>2. L'entité a-t-elle mis en place des procédures en matière de sécurité pour l'identification et l'authentification des utilisateurs autorisés ?</p> <p>3. L'entité a-t-elle mis en place des procédures pour permettre aux utilisateurs de modifier, de mettre à jour ou d'éliminer leur propre profil d'utilisateur ?</p> <p>4. L'entité a-t-elle mis en place des procédures visant à limiter l'accès à distance au réseau interne au personnel autorisé ?</p> <p>5. L'entité a-t-elle mis en place des procédures visant à protéger les systèmes internes contre les virus et les programmes malveillants ?</p> <p>6. L'entité a-t-elle mis en place des procédures visant à empêcher des clients, des groupes de personnes ou d'autres entités d'accéder à des renseignements personnels ou sensibles autres que les leurs d'une façon qui pourrait nuire à l'accessibilité ?</p> <p>7. L'entité a-t-elle mis en place des procédures visant à limiter l'accès (qui pourrait nuire à l'accessibilité) aux systèmes et aux données aux seuls employés autorisés, en fonction des rôles et des responsabilités qui leur sont confiés ?</p> <p>8. L'entité utilise-t-elle le chiffrement ou d'autres mesures de sécurité équivalentes pour éviter que les renseignements concernant l'authentification et la vérification des utilisateurs soient interceptés lors de leur transmission sur Internet ?</p> <p>9. L'entité a-t-elle mis en place des procédures visant à maintenir des configurations de systèmes qui minimisent les problèmes d'accessibilité et les risques pour la sécurité correspondants ?</p> <p>10. L'entité a-t-elle mis en place des procédures qui lui permettent de surveiller les brèches de sécurité qui nuisent à l'accessibilité, et d'agir en conséquence ?</p> <p><i>Contrôles précis relatifs à l'accessibilité</i></p> <p>11. L'entité a-t-elle pris en compte les questions d'environnement liées à l'accessibilité et le système est-il protégé contre les menaces susceptibles d'interrompre son fonctionnement et de nuire à son accessibilité ?</p> <p>12. L'entité a-t-elle mis en place des procédures pour surveiller l'accessibilité et la capacité par rapport à l'engagement indiqué et pour prévoir les besoins futurs ?</p> <p>13. Est-ce que l'entité documente, autorise, met à l'essai et approuve les</p>				
<p>modifications proposées aux systèmes avant leur mise en oeuvre, de façon à protéger l'accessibilité de son/ses système(s) de commerce électronique ?</p> <p>14. Est-ce que l'entité documente et autorise les modifications apportées en situation d'urgence (y compris après l'événement) ?</p> <p>15. L'entité prévoit-elle des processus de sauvegarde, de stockage hors place et de</p>				

restauration et des plans antisinistre qui lui permettent de respecter l'engagement indiqué quant à l'accessibilité ? 16. L'entité protège-t-elle l'intégrité des copies des données et des informations qui sont conservées afin de respecter ses engagements quant à l'accessibilité qui sont indiqués dans son site Web ?				
> Surveillance 1. L'entité a-t-elle mis en place des procédures pour surveiller l'accessibilité de ses systèmes de commerce électronique et relever les modifications à apporter aux contrôles relatifs à l'accessibilité et à la sécurité ? 2. L'entité a-t-elle mis en place des procédures pour surveiller sa politique en matière d'accessibilité et d'atteinte à la sécurité pour la mettre à jour au besoin, en fonction de l'évolution technologique, des modifications apportées à la structure du/des système(s) de commerce électronique ou d'autres informations ? 3. L'entité a-t-elle mis en place des procédures visant à surveiller les changements environnementaux et technologiques, ainsi que les risques correspondants et leur incidence sur le plan antisinistre ? 4. L'entité a-t-elle mis en place des procédures pour s'assurer que les rapports de non-conformité aux informations et aux contrôles relatifs à l'accessibilité sont pris en considération et que des correctifs sont apportés régulièrement et rapidement ?				

8. Check-list pour le principe relatif à la confidentialité :

<i>Check-list pour l'évaluation du contrôle interne pour le principe de confidentialité</i>	O	N	N/A	WP REF
> Informations 1. L'entité décrit-elle pratiques en matière de confidentialité, avant que l'information confidentielle ne soit fournie, notamment: a. La façon dont l'information est qualifiée de confidentielle ou cesse de l'être ; b. La façon dont l'accès à l'information confidentielle est autorisé ; c. La façon dont l'information confidentielle est utilisée ; d. La façon dont l'information confidentielle est partagée ; e. si l'entité transmet l'information à des tiers, est-il mentionné toute limite quant à la mesure dans laquelle elle se fie aux pratiques et contrôles de ces tiers en matière de confidentialité ? Sinon, l'entité indique-t-elle qu'elle se fie aux pratiques et contrôles de ces tiers qui sont équivalents ou supérieurs aux siens ? f. La référence aux textes et lois relatifs à la confidentialité et l'indication de leur respect par l'entité 2. L'entité décrit-elle l'information communiquée par l'entité aux particuliers, aux entreprises et aux autres utilisateurs pour permettre à ceux-ci de l'informer au sujet de brèches réelles ou possibles à la confidentialité des données et à la sécurité de son ou ses systèmes connexes ? 3. L'entité indique-t-elle aux clients les canaux permettant de poser des questions ou d'obtenir de l'aide ? 4. L'entité décrit-elle les procédures mises en place par l'entité pour résoudre les différends, y compris au minimum les suivantes : a. Procédures à suivre pour régler les plaintes, d'abord avec l'entité. b. Résolution des plaintes relatives à l'exactitude, à l'intégralité et à l'utilisation des informations confidentielles Utilisation qui sera faite des renseignements confidentiels faisant l'objet de la plainte ou mesures qui seront prises à leur				
égard, jusqu'au règlement satisfaisant de la plainte. c. Engagement de la direction à recourir à un service de règlement des différends offert par un tiers désigné à cette fin, s'il s'avère que le client n'est pas entièrement satisfait du règlement proposé par l'entité à l'égard de la plainte. d. Engagement de ce tiers à régler les plaintes non réglées ? 5. L'entité indique-t-elle le processus utilisé pour définir et communiquer les				

<p>modifications ou mises à jour de ses pratiques en matière de confidentialité et de ses pratiques de sécurité connexes?</p>				
<p>> Politiques</p> <ol style="list-style-type: none"> 1. L'entité a-t-elle une politique en matière de protection des informations confidentielles ou secrètes, notamment les éléments suivants : <ol style="list-style-type: none"> a. Qui a l'autorisation d'accès, quelle est la nature de cet accès et qui l'autorise ? b. Procédures pour ajouter de nouveaux utilisateurs, modifier les niveaux d'accès des utilisateurs actuels et retirer l'accès aux utilisateurs qui n'en ont plus besoin ? c. Façon dont les plaintes relatives à la confidentialité des données peuvent être traitées ? d. Procédures pour traiter les atteintes à la sécurité ? e. Les contrôles à l'égard des accès physiques aux systèmes ? j. D'autres procédures de sécurité relatives à la protection des informations confidentielles ? 2. Existe-t-il des procédures permettant aux responsables de la protection des données confidentielles d'être mis au courant de la politique publiée par l'entité en la matière et des politiques de sécurité connexes, et de suivre le respect de ces politiques ? 3. Les responsabilités de la politique en matière de confidentialité de l'information et des politiques de sécurité connexes ont-elles été clairement confiées ? 4. Existe-t-il des procédures de formation et des ressources visant à appuyer la politique en matière de protection des informations confidentielles et les politiques de sécurité connexes ? 5. Y a-t-il des procédures employées pour évaluer si la politique en matière de protection des données confidentielles et les politiques de sécurité connexes de l'entité correspondent à ses pratiques déclarées et aux lois et règlements en vigueur ? 				
<p>> Procédures</p> <p><i>Critères de sécurité relatifs à la confidentialité:</i></p> <ol style="list-style-type: none"> 1. Existe-t-il des procédures de sécurité visant les nouveaux utilisateurs ? 2. Y a-t-il des procédures permettant d'identifier et d'authentifier les utilisateurs autorisés ? 3. Existe-t-il des procédures permettant aux utilisateurs de modifier, de mettre à jour et de supprimer leur propre profil ? 4. Les procédures permettent-elles de réserver aux employés autorisés l'accès à distance au réseau ? 5. Y a-t-il des procédures de nature à empêcher des clients, des groupes de personnes ou d'autres entités d'accéder à des renseignements confidentiels ou secrets autres que les leurs ? 6. L'accès aux informations confidentielles est-il restreint aux seuls employés autorisés, selon les rôles et les responsabilités qui leur sont confiés ? 7. Les programmes et les données sont-ils protégés pendant le processus de sauvegarde, de stockage ou de restauration ? 8. L'entité utilise-t-elle le chiffrement à 128 bits au minimum pour éviter que l'authentification, la vérification et les données confidentielles ou secrètes soient interceptées par des destinataires non souhaités lors de leur transmission sur 				
<p>Internet ?</p> <ol style="list-style-type: none"> 9. Existe-t-il des procédures visant à maintenir des configurations de système qui minimisent les risques susceptibles de compromettre la sécurité des informations confidentielles ? 10. Les brèches de sécurité sont-elles surveillées par des procédures permettant d'agir pour stopper ou limiter les risques ? <p><i>Critères propres à la confidentialité :</i></p>				

<p>11. Existe-t-il des contrôles et procédures visant à assurer que l'information confidentielle obtenue dans le cadre d'une opération de commerce électronique n'est communiquée qu'aux parties en cause, conformément à ses pratiques déclarées en matière de confidentialité ?</p> <p>12. L'entité acquiert-elle l'assurance, ou une déclaration selon laquelle en ce qui concerne les tiers auxquels est transmise l'information, les politiques en matière de confidentialité sur lesquelles s'appuie l'entité sont en conformité avec ses pratiques déclarées en matière de confidentialité ?</p> <p>13. Si les politiques déclarées en matière de confidentialité sont supprimées ou deviennent moins restrictives, l'entité garde-t-elle les anciennes procédures pour protéger les anciennes informations confidentielles obtenues ? Sinon, obtient-elle l'autorisation de son partenaire commercial pour appliquer de nouvelles procédures moins restrictives à des informations confidentielles obtenues avant leur application ?</p>				
<p>> Surveillance</p> <p>1. Existe-t-il des procédures de surveillance relatives à la sécurité des systèmes de commerce électronique, permettant en plus de relever les modifications à apporter aux contrôles sur la confidentialité ?</p> <p>2. L'entité a-t-elle mis en place des procédures pour surveiller les changements environnementaux et technologiques ainsi que les risques connexes, afin de garder ses pratiques déclarées en matière de confidentialité et les politiques afférentes conformes et à jour avec les lois et règlements ?</p> <p>3. L'entité a-t-elle mis en place des procédures pour surveiller sa politique en matière d'atteinte à la sécurité et la mettre à jour au besoin pour tenir compte de l'évolution technologique, des modifications apportées à la structure des systèmes de commerce électronique, ou d'autres informations ?</p> <p>4. L'entité dispose-t-elle de procédures pour surveiller les cas de non-conformité aux informations sur la confidentialité et la sécurité, et apporter les correctifs nécessaires régulièrement et rapidement ?</p>				

Les points forts de contrôle qui ressortent des questionnaires doivent être testés et validés. Pour ce, l'expert comptable déploie un ensemble de procédures incluant des observations, des enquêtes, des essais et, surtout, des tests de conformité et d'application. En effet, si les observations, enquêtes et essais permettent d'attester de l'existence du contrôle, les tests de conformité et d'application sont le garant de leur efficacité et de la permanence de leur exécution. La réalisation des tests de conformité et d'application s'appuie principalement sur la réalisation de sondages et d'échantillonnage sur les opérations et les transactions de e-commerce. Ces tests de conformité et d'application aboutissent donc à une évaluation des points forts de contrôle interne et, par conséquent, à une appréciation du risque de contrôle. Le vérificateur peut conclure sur le niveau de ce risque en le plaçant dans des catégories linguistiques (faible, modéré, élevé...) correspondant chacune à une probabilité de risque que les contrôles internes ne détectent pas des erreurs ou des incidents liés aux transactions.

A partir de cette évaluation du système de contrôle interne lié à un site, et celle du risque inhérent présentée dans un précédent dossier, c'est le métier de l'expert comptable et les standards régissant sa profession qui prennent le relais pour en faire l'usage pertinent qui s'impose au niveau de la direction de la mission, la planification des travaux et leur exécution, afin d'aboutir à la formation d'une opinion juste, solide et justifiable dans tous ses aspects significatifs.

Nabil Ghodhbane
Expert comptable