

## **Considérations pour l'évaluation du risque de contrôle lié à l'activité du site e-commerce (Partie 1)**

Dans la continuité du dossier de la semaine précédente consacré à un modèle d'évaluation du risque inhérent lié à l'activité d'un site de e-commerce, nous proposons cette semaine d'approfondir l'analyse au deuxième niveau, dans l'équation de l'auditeur, incarné par le risque de contrôle.

### **A. Le contrôle interne et le paradigme de gestion des risques**

Le paradigme de gestion des risques<sup>1</sup> est un modèle qui reconnaît que la gestion des risques est un processus continu et dynamique et non pas un événement annuel ou biennuel. Ce processus est composée de cinq étapes successives et enchevêtrées :

- Première étape : l'identification et le scannage de l'environnement interne et externe afin d'identifier les risques liés aux technologies de l'information avant qu'ils deviennent actifs. Même si l'attitude réactive est parfois inévitable, le modèle de gestion des risques préconise de minimiser les solutions réactives au profit d'une architecture de contrôle proactive devant les risques ;
- Seconde étape : l'analyse des risques identifiés par l'examen de leur probabilité de réalisation et leurs impacts potentiels. Dans cette étape, tous les risques identifiés doivent être classés par nature (risque de continuité d'activité, vol de données, pertes d'informations...) et répertoriés selon leur urgence et leur priorité,
- Troisième étape : la planification qui consiste en l'évaluation des ressources humaines et matérielles à la disposition de l'entité et leur allocation aux catégories de risques identifiés et répertoriés. Dans certains cas, les entités s'aperçoivent à ce stade de l'insuffisance ou de l'inadéquation de leurs moyens et décident d'affecter des ressources additionnelles afin de boucler leur plans de gestion des risques liés aux technologies d'information,
- Quatrième phase : la surveillance de l'exécution du plan arrive ensuite pour assurer que les actions planifiées sont exécutées comme prévu et que toute exception est suivie et traitée à part. La surveillance implique aussi le suivi continu des indicateurs de risques et la signalisation de toute exception ou disproportion dans ces indicateurs,
- Cinquième étape : le contrôle des données de la quatrième phase pour mettre en exécution des actions correctives. Cette phase est étroitement liée à la surveillance dans la mesure où elle s'en trouve directement alimentée et enclenchée par ses « drapeaux d'alerte ».

Le plus important est de noter que ce processus est itératif dans la mesure où les phases d'identification, d'analyse ou de surveillance peuvent toujours identifier de nouveaux risques et induire la planification de leur traitement et leur contrôle. La flexibilité et la fluidité des canaux d'information et de feedback sont donc les maîtres mots dans un modèle de gestion des risques.

Cette présentation du modèle de gestion des risques n'est pas sans rappeler la structure fondamentale d'un système de contrôle interne telle qu'établie par le COSO<sup>2</sup>. En effet, les éléments d'un système de contrôle interne comprennent l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication et, enfin, la surveillance. Ces éléments qui retracent la géométrie du paradigme de gestion des risques, aboutissent à faire

---

<sup>1</sup> Adapté du « *Risk Management Paradigm* » élaboré par le SEI (*Software Engineering Institute*)

<sup>2</sup> COSO, *Committee of Sponsoring Organizations of the Treadway Commission*

d'un bon système de contrôle interne la solution de l'organisation au filtrage et à la négociation de ses risques.

Par conséquent, il est important de considérer les éléments constitutifs de tout système de contrôle interne dans l'évaluation des contrôles d'un système de e-commerce. Cette évaluation sera matérialisée au niveau des questionnaires de contrôle interne proposés dans ce dossier. Auparavant, il est aussi important de souligner les structures spécifiques des contrôles internes d'un système de commerce électronique orienté transactions afin de mieux appréhender leur évaluation.

### **B. Structure des contrôles internes sur les transactions dans un système de e-commerce**

Accoutumé aux systèmes traditionnels de contrôle interne dans une transaction de vente classique, l'expert comptable doit cerner certaines subtilités relatives aux transactions de vente dans un système de e-commerce. Le souci majeur de l'expert comptable, que ce soit dans une transaction de vente traditionnelle ou sur un système de e-commerce, reste l'intégrité de la transaction, c'est-à-dire son exhaustivité, son exactitude, sa ponctualité et son autorisation.

Pour la vérification de l'intégrité des opérations, l'évaluation du système de contrôle interne est largement dépendante de l'appréciation de la fiabilité du système dans la capture et le traitement des informations liés à une transaction de vente. Dans un système de e-commerce assez sophistiqué, la première étape de la transaction, telle que la réception d'une commande client en ligne, est le fait générateur à un traitement automatique des autres étapes ultérieures de cette transaction. Ainsi, si dans une transaction de vente traditionnelle l'expert comptable peut s'attarder à évaluer les contrôles lors de chaque étape du processus de vente de façon séparée, il ne peut se permettre cette partition dans une transaction de e-commerce. Là, l'expert comptable doit concentrer son évaluation sur les contrôles automatisés assurant l'intégrité de la transaction au fur à mesure de leur saisie et leur traitement immédiat et automatique.

Les contrôles liés à l'intégrité des transactions de vente dans un environnement de e-commerce sont souvent dessinés de façon à :

- Valider l'entrée,
- Prévenir toute omission, ou duplication, de la transaction,
- S'assurer que les conditions et les termes de la vente ont été acceptés avant son traitement automatisé. Ceci peut requérir, par exemple, que le paiement soit effectué et obtenu au moment de la commande,
- Distinguer entre un client naviguant sur le site et un client plaçant ses commandes, en s'assurant que le client ayant rempli son panier et confirmé sa commande ne peut dénier la transaction ou ses termes (non répudiation), et en vérifiant dans certains cas que la transaction se fait avec des parties approuvées,
- Traiter les problèmes qui peuvent faire échouer la transaction, tels que les interruptions d'alimentation ou de connexion (du côté du site ou du client), les échecs d'authentification des cartes de crédit ou des moyens de paiement ou ceux de communication entre le moment d'envoi de l'autorisation et celui de réception de la réponse,
- Prévenir un traitement incomplet en s'assurant que toutes les étapes sont remplies (dans l'exemple d'une vente B to C : la commande est acceptée, le paiement est reçu, les biens et services sont livrés et les différents systèmes de suivi, de gestion et de journalisation sont mis à jour). Dans le cas contraire, les contrôles doivent aboutir à rejeter la commande,
- Assurer une distribution systématique et adéquate des données de la transaction aux

différents systèmes concernés (magasin, facturation, paiement, livraison, finance et comptabilité...),

- Assurer que les enregistrements et les journaux sont convenablement et systématiquement maintenus et actualisés.

Outre ces contrôles sur l'intégrité de la transaction, les contrôles internes automatisés doivent permettre la fluidité et la non rupture dans le processus de traitement. Ces contrôles traitent la façon dont des systèmes de e-commerce sont intégrés les uns avec les autres et opèrent ainsi comme un système unique. La partie apparente d'un site Web cache, en effet, une multitude de systèmes, appelés « back-office », qui peuvent être composés de :

- système de gestion des commandes,
- système de gestion des inventaires,
- systèmes de gestion de profils,
- Systèmes de gestion des livraisons
- système de gestion des paiements.

Les contrôles qui permettent l'intégration et l'interfaçage de ces systèmes doivent aussi être évalués et testés. D'ailleurs, plusieurs sites Web ne sont pas automatiquement intégrés à leurs systèmes de back office, et doivent passer par une interface manuelle pour collecter les ordres, les trier, les dispatcher et les exécuter. De pareils cas constituent une source de risque au niveau de l'intégrité et de l'intégration des transactions et requièrent des diligences particulières de la part de l'expert comptable.

### **C. Questionnaires et programmes de travail pour l'évaluation des risques de contrôle**

Dans ce paragraphe, nous allons proposer des questionnaires d'évaluation des contrôles internes d'un système de commerce électronique. Ces questionnaires sont donnés à titre indicatif et non limitatif et ne peuvent se substituer à ceux rédigés sur la base de la compréhension, l'expérience et le jugement professionnel de l'expert comptable.

Ces questionnaires s'attaquent à plusieurs aspects couverts par les contrôles internes d'un système de e-commerce. Ils sont construits de façon à évaluer les systèmes de contrôle interne en général, puis ceux particuliers à un système informatisé, puis ceux spécifiques à un système de e-commerce, pour finir avec ceux singuliers aux principes et critères spécifiques de sécurité, de confidentialité et d'intégrité des transactions. Ainsi, ces questionnaires sont subdivisés en quatre parties, allant du général au particulier, et s'attardant respectivement sur :

- A. L'évaluation des éléments constitutifs d'un système de contrôle interne : c'est un tronc commun à tous les systèmes de contrôle interne (pas seulement ceux liés au e-commerce) et couvre l'évaluation de l'environnement de contrôle, de l'évaluation des risques, des procédures de contrôle, des information et communication et de la surveillance,
- B. L'évaluation des contrôles généraux du système informatique : il s'agit d'une évaluation spécifique aux systèmes bâtis sur des structures et des moyens informatisés, y compris les systèmes de e-commerce,
- C. L'évaluation des sécurité et des contrôles du serveur Web et de l'infrastructure matérielle et logicielle utilisée par le système de e-commerce,
- D. L'évaluation des contrôles internes garantissant le respect des principes et critères généralement admis en matière de sécurité, de confidentialité et d'intégrité des transactions.

## 1. Questionnaire de contrôle interne pour l'évaluation des composants du contrôle interne :

<b>Questionnaire pour l'évaluation des composants du contrôle interne</b>	<b>O<sup>3</sup></b>	<b>N<sup>4</sup></b>	<b>N/A<sup>5</sup></b>	<b>WP REF<sup>6</sup></b>
<p><b>1) L'environnement de contrôle :</b>            Il donne le ton sur la solidité d'une organisation et influence activement la conscience du contrôle chez ses membres. C'est la base fondamentale pour tous les composants du contrôle interne et le fournisseur en discipline et en structure. C'est le produit de l'attitude, la conscience et des actions du management senior, des propriétaires, du conseil d'Administration ou de tout fondé de pouvoir au sein de l'entreprise. Leur action se traduit par la communication, explicite ou implicite, aux autres membres de l'organisation, leur philosophie à propos de l'importance du contrôle et du poids que ce dernier doit avoir dans l'entité :</p>				
<p><i>Intégrité et valeurs éthiques :</i>            - Sur la base de votre expérience passée ou sur les investigations sur le client, il apparaît que les hauts responsables et employés semblent être honnêtes.            - Quelques preuves sur la possible implication des hauts responsables ou employés dans des conduites douteuses de faible valeur éthique ont été amenées à notre attention (de plus amples renseignements sont requis).            - Les recrutements des hauts responsables sont précédés par des investigations sur leurs références et leur passé.            - Les employés sont encouragés à reporter les inconvenances suspectes aux hauts responsables.            - Le client possède un code écrit de conduite, ou autres procédures écrites, sur les pratiques, la conduite et l'opposition des intérêts.</p>				
<p><i>Respect des compétences :</i>            - Les politiques et pratiques relevées concernant la gestion des ressources humaines, l'affectation de l'autorité et des tâches, l'interaction entre la direction et les employés clé, indiquent que le degré de respect des compétences par la direction lors de l'affectation des responsabilités est :            1. Elevé            2. Faible</p>				
<p><i>Implication des organes de direction :</i>            - L'organe de direction du client est exclusivement composé des hauts responsables clé.            - Le client dispose d'un organe de direction actif avec des membres qualifiés, non impliqués dans la gestion, s'engagent régulièrement dans la revue des activités financières et autres de la société</p>				
<p><i>Philosophie de la direction et style de gestion :</i>            - La Direction participe dans les opérations quotidiennes et approuve les transactions larges ou non courantes.            - La Direction comprend, évalue, demande ou utilise des rapports financiers ou autres formes d'information financière dans sa gestion courante des affaires.            - Le risque d'activité toléré par la Direction est jugé :            1. Elevé            2. Faible            - La Direction est orientée vers ses buts et objectifs, et ces derniers sont jugés :            1. Prudents et raisonnablement réalisables            2. Ambitieux et probablement excessifs            - Concernant sa responsabilité d'énoncer et de respecter ses pratiques en matière de e-commerce, la Direction semble être :            1. Conservatrice et appliquée.            2. Agressive et peu respectueuse.</p>				

<sup>3</sup> Oui

<sup>4</sup> Non

<sup>5</sup> Non Applicable

<sup>6</sup> WorkPaper Reference, référence du papier de travail

<b>Questionnaire pour l'évaluation des composants du contrôle interne</b>	<b>O<sup>7</sup></b>	<b>N<sup>8</sup></b>	<b>N/A<sup>9</sup></b>	<b>WP REF<sup>10</sup></b>
- Le style de management peut être décrit, plutôt : 1. Participatif et communicatif, orienté vers le travail d'équipe et le développement, 2. Autocratique, renfermé et étouffant.				
<i>Structure organisationnelle :</i> - Selon la taille et la complexité de ses opérations de e-commerce, la structure organisationnelle du client, dans sa globalité ou pour celle liée aux opérations de e-commerce, semblent être : 1. Appropriée 2. Indûment complexe 3. Surchargée par insuffisance de niveaux de management - Le client dispose d'un directeur des technologies d'information (IT) qualifié, dont l'autorité ne dérive pas de celle des autres directeurs ou organes de direction.				
<i>Affectation des responsabilités et de l'autorité :</i> - L'autorité et la responsabilité dans la prise de décision est clairement apparente, périodiquement communiquée et convenablement ventilée dans les différents niveaux du management, eu égard aux participations, à la structure organisationnelle et à la complexité de l'activité du client. - L'autorité et la responsabilité, particulièrement pour les fonctions liées au système				
d'information et aux activités de e-commerce, apparaissent clairement et sont périodiquement communiquées et convenablement affectées eu égard à la spécificité du client. - Le client dispose d'un organigramme formel, et de procédures écrites (manuel ou autres), actualisés, définissant les rôles, fixant les responsabilités et déléguant des degrés d'autorité dans l'approbation et l'exécution transactions.				
<i>Procédures et pratiques pour les ressources humaines :</i> - La Direction et les hauts cadres participent activement dans le recrutement, la formation, l'évaluation ou la promotion du personnel. - Le personnel ayant accès aux actifs précieux, aux données et systèmes sensibles, ou ceux dans une position de confiance, sont convenablement retenus et payés. - Les niveaux de salaire et de performance, la charge du travail, les taux de rotation, la qualité et la fréquentation des programmes de formation, les procédures de revue des travaux des subordonnés et les autres éléments observés, indiquent et assurent un travail satisfaisant par les cadres ordinaires et les subordonnés (particulièrement pour le personnel des technologies de l'information ou celui impliqué dans le système d'information). - Le client dispose d'un système de recrutement formel et satisfaisant pour les employés impliqués dans la technologie de l'information ou les opérations de e-commerce. - Le client dispose d'un système d'évaluation des performances, capable de distinguer les candidats qualifiés pour la promotion.				
<b>2) L'évaluation des risques :</b>  Le processus d'évaluation du risque lié aux activités de e-commerce concerne la façon dont le management identifie et traite les risques, internes et externes, que ses opérations de e-commerce ne soient pas en conformité avec les bonnes pratiques généralement admises et recommandées en matière de e-commerce . Ces risques incluent ceux inhérents aux activités de l'entité, ou ceux nés d'une transaction inhabituelle, importante ou spécifique, ceux liés à une modification dans l'environnement d'exploitation, le personnel, la technologie, la ligne de produits, ou la taille de l'entreprise. Cette composante du risque est d'autant plus importante que l'environnement de l'entreprise est instable (elle est moins signifiante pour un environnement stable)				

<sup>7</sup> Oui

<sup>8</sup> Non

<sup>9</sup> Non Applicable

<sup>10</sup> WorkPaper Reference, référence du papier de travail

<b>Questionnaire pour l'évaluation des composants du contrôle interne</b>	<b>O</b>	<b>N</b>	<b>N/A</b>	<b>WP REF</b>
<p>- La Direction et le personnel IT s'engagent fréquemment et informellement dans l'évaluation des facteurs de risques internes et externes et préconisent des améliorations au contrôle interne quand nécessaire.</p> <p>- La Direction compte, en premier, sur les auditeurs externes ou les réviseurs pour attirer à son attention les risques relatifs aux activités de e-commerce</p>				
<p>et qui exigent une amélioration du contrôle interne ou une formation pour le personnel concerné.</p>				
<p>- Le client dispose d'un système d'évaluation des risques internes et externes liés aux activités de e-commerce dus aux changements dans les circonstances et nécessitant une amélioration du contrôle interne ou une formation formelle ou informelle du personnel</p>				
<p><b>3) Activités de contrôle :</b></p> <p>Les activités de contrôle concernent la politique et les procédures utilisées pour fournir une assurance raisonnable que les directives du management sont prises afin d'atteindre les objectifs de l'entité. Ceux afférents aux activités de e-commerce incluent les procédures liées au système de e-commerce et peuvent être rattachés aux contrôles généraux et aux contrôles des applications. Ceux liés aux pratiques de e-commerce et à la conformité avec les principes et critères généralement admis et recommandés.</p> <p>Les procédures de contrôle peuvent être classées dans les 4 catégories suivantes : (a) évaluations des performances, (b) processus d'information, (c) contrôles physiques et (d) séparation des tâches.</p>				
<p>NB :</p> <p>1- Les questionnaires sur les contrôles généraux, les contrôles d'application, les contrôles sur l'infrastructure Web seront exposés en détail aux paragraphes 1.1.3 et 1.1.4 ci-après</p> <p>2- Les questionnaires sur les contrôles liés aux pratiques de e-commerce et leur conformité aux principes et critères généralement admis et recommandés seront détaillés après ce questionnaire général sur l'évaluation des composants du contrôle interne</p>				
<p>- Le client a établi une politique et des procédures d'autorisation des transactions aux niveaux appropriés du management.</p> <p>- La structure organisationnelle du client est telle que la ségrégation des tâches incompatibles est optimale et que ces tâches en soient exclues.</p> <p>- Les procédures de contrôle effectuées sont matérialisées par des visas, des signatures, des sceaux, des confirmations ou toute autre procédé permettant de justifier leur existence et leur application.</p> <p>- Les procédures de contrôle sont journalisées et conservées un certain moment afin de permettre leur vérification ultérieure ou la traçabilité des responsabilités.</p>				
<p><b>4) Information et communication</b></p> <p>De bons canaux de communication doivent exister pour assurer la distribution des informations relatives à l'identification, l'analyse et le traitement des risques au personnel approprié. Grâce à la communication, un feedback est établi et des actions correctives ou proactives peuvent être prises en temps opportun et de façon pertinente et efficace.</p>				
<p>- Le client met à la disposition de son personnel, un manuel de procédures, ou autres documentation écrite équivalente, qui répand, décrit et commente les procédures de contrôle interne aux responsables pour l'accomplissement de leurs tâches.</p> <p>- Des canaux de communication et de coordination existent entre les divers départements et personnes impliquées dans les opérations de e-commerce. Ces canaux sont fonctionnels, rapides et pertinents et permettent de véhiculer la bonne information à la bonne personne et recevoir un feedback.</p>				

<b>Questionnaire pour l'évaluation des composants du contrôle interne</b>	<b>O</b>	<b>N</b>	<b>N/A</b>	<b>WP REF</b>
<p><b>5) Surveillance :</b></p> <p>La surveillance concerne les moyens mis en œuvre par la Direction afin d'évaluer périodiquement l'architecture et l'applicabilité du contrôle interne, ainsi que les actions correctives qu'il engendre.</p>				
<ul style="list-style-type: none"> <li>- Le personnel est encouragé à reporter informellement les déficiences relevées dans le système de contrôle interne, ainsi que toute suggestions d'amélioration.</li> <li>- La Direction compte principalement sur ses auditeurs externes ou les vérificateurs pour lui attirer son attention sur des faiblesses, des améliorations, de la non conformité au contrôle interne observés durant les missions.</li> <li>- Le client possède un processus d'évaluation, à travers le temps, de la pertinence de l'architecture de son système de contrôle interne et de son adaptation aux exigences et aux risques des activités de e-commerce.</li> <li>- Les organes de direction s'impliquent régulièrement dans des activités de surveillance du système de contrôle interne lié aux activités de e-commerce.</li> <li>- Le client dispose d'une fonction d'audit interne qui n'est pas limitée à l'audit des activités d'exploitation, mais inclut aussi les activités significatives et continues relevant du système de e-commerce et, particulièrement, la surveillance du contrôle interne y afférent.</li> </ul>				

A la suite de ce questionnaire général sur l'évaluation des composants du système de contrôle interne, l'expert comptable abordera l'évaluation plus spécifique à l'activité de e-commerce du site que nous présenterons au dossier de la semaine prochaine.

Nabil Ghodhbane  
Expert comptable membre de l'ordre