

## **Modèle d'évaluation du risque inhérent lié à l'activité du site e-commerce**

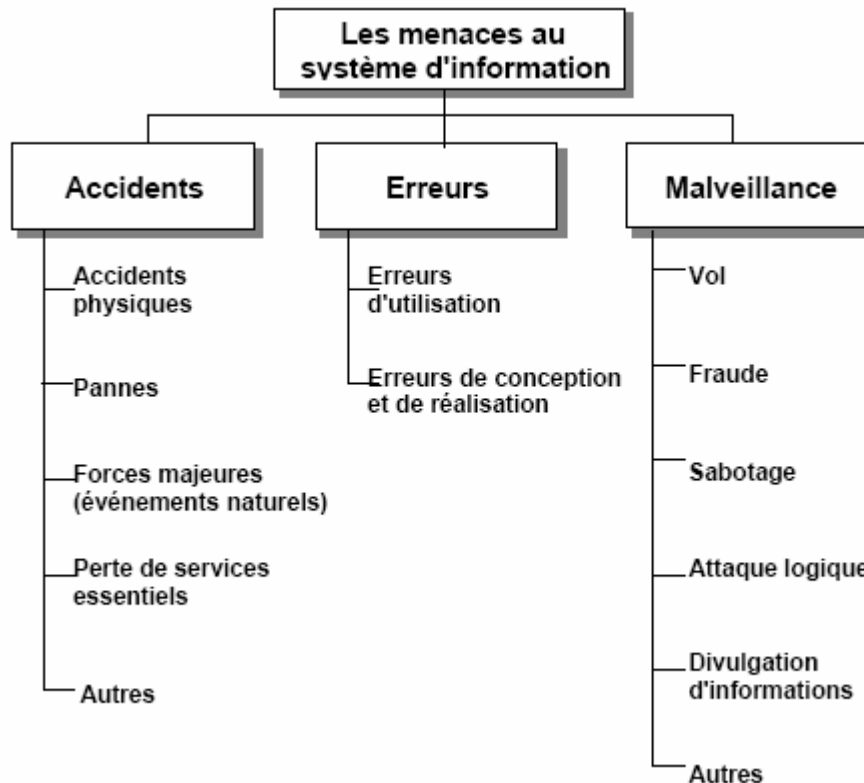
### ***A. Identification des risques inhérents liés à l'activité de e-commerce du site***

Si les activités liées au e-commerce ont fait apparaître de nouveaux types de risques, dans un grand nombre de cas ce sont des risques classiques qui se trouvent démultipliés et amplifiés par le recours à ce média nouveau que constitue l'Internet. Ainsi, il n'y a pas de véritables risques inhérents standard liés au e-commerce, et les expositions aux risques varieront en fonction l'activité du site, du sérieux de sa direction et des systèmes utilisés.

Néanmoins, on peut mettre en évidence un certain nombre de facteurs de risques inhérents et corrélativement des impacts spécifiques, parmi lesquels nous citons :

- Dépendance à une technologie complexe qui peut être fragile et insuffisamment testée pour sa tolérance aux défauts. Dans un secteur où il faut « devancer » ses concurrents, ce facteur peut s'avérer important,
- Infrastructure décentralisée de l'Internet et multiplicité des intervenants,
- Concentration d'activités et de services qui étaient auparavant éclatés, voire externalisés (tels que la publicité, la livraison, le paiement,...),
- Nécessité technique de connecter des systèmes internes critiques au monde extérieur (par exemple, le contrôle des commandes et des inventaires, la comptabilité et paiement, les systèmes de contrôle d'accès, les systèmes d'identification et d'authentification,...),
- Extension de la législation du droit d'auteur aux logiciels, au contenu et aux applications commerciales et la fréquence accrue des litiges fondés sur le droit d'auteur de nature complexe dans le monde,
- Nécessité technique d'acquérir de la technologie à l'extérieur de l'entreprise. Ces prestataires externes peuvent être sous capitalisés et financièrement insolubles, entraînant des risques de conflit d'intérêt ou de difficulté dans la répartition ou la gestion des risques,
- Risque accru de fraude technologique : défis de hacking (ou piratage) des sites connus ou fortement protégés,
- Evolution de plus en plus perceptible des actifs matériels vers des actifs immatériels : la notion de valeur est en train de migrer vers l'immatériel, rendant ces actifs plus convoités,

Etant des systèmes bâtis sur des structures de systèmes d'information, les systèmes de e-commerce subissent les mêmes menaces classifiées dans le schéma suivant :



Parmi les autres impacts spécifiques de ces risques inhérents se trouvent les suivants :

- Evolution de la sinistralité vers des pertes pécuniaires et des préjudices immatériels :
  - . Introduction et transmission non intentionnelles de virus ou de données ou codes défectueux,
  - . Divulgence non autorisée de données confidentielles de clients ou partenaires,
  - . Défaut ou arrêt de connexion provoquant des dommages aux tiers qui dépendent d'un service ininterrompu.
- Aggravation des risques de pertes d'exploitation consécutives à des dommages immatériels :
  - . Défaillance du logiciel e-commerce due à des erreurs de conception, de développement, de paramétrage et d'administration,
  - . Panne des systèmes internes et externes,
  - . Malveillance informatique ou accès non autorisé au système,
  - . Négligence dans la mise à jour, le maintien ou l'utilisation des bases de données et systèmes informatiques,
  - . Vol, détournement de propriété intellectuelle (droit d'auteur, marques déposées ...),
  - . Non respect des modalités d'usage de technologies appartenant à des tiers.
- Aggravation des risques d'atteinte à des actifs ou biens immatériels :
  - . Vol de services,
  - . Violation des droits de propriété intellectuelle,
  - . Vol d'informations confidentielles,
  - . Dommages et pertes ou diffusion de données accidentels par des employés.
- Du fait de l'importance donnée au contenu, augmentation significative du risque direct et indirect de responsabilité publicitaire ou éditoriale.

Compte tenu de ces menaces, de leurs facteurs et impacts, le risque inhérent pour la plupart des systèmes de e-commerce est normalement élevé, car les erreurs potentielles couvrent généralement aussi, plusieurs systèmes et, utilisateurs et intervenants. Dans son évaluation du risque inhérent lié aux activités de e-commerce du site, l'expert considère aussi bien les risques inhérents généraux que ceux spécifiques. Les premiers sont inhérents à toute activité et sont ceux évalués par tout expert dans une mission d'audit financier classique, alors que les seconds sont spécifiques aux systèmes bâtis sur des infrastructures informatiques et liés à la complexité technologique, l'étendue des systèmes et les changements dans les processus.

**«...le risque inhérent pour la plupart des systèmes de e-commerce est normalement élevé, car les erreurs potentielles couvrent généralement plusieurs systèmes et, aussi, plusieurs utilisateurs et intervenants... »**

Au niveau des risques inhérents généraux, les facteurs suivants doivent être considérés :

- l'intégrité, la compétence et l'expérience de la direction du site,
- les changements dans la direction du site,
- les pressions sur la direction (concurrence, clients, pirates...),
- la nature de l'organisation des systèmes et des activités (complexité des systèmes, leur degré d'intégration...),
- les facteurs touchant au secteur d'activité dans l'ensemble (changements technologiques, concurrence...),
- le degré d'implication des tiers sous-traitants dans le système de e-commerce (externalisation des services d'hébergement, de sécurité, de développement...),
- Les conclusions, constatations et trouvailles des précédentes vérifications ou audits des systèmes informatiques de l'entité.

Au niveau des risques inhérents spécifiques, d'autres questions sont à considérer, dont :

- les conclusions et constatations des précédents audits ou vérifications du système informatique,
- les intervalles entre chaque revue du système,
- la complexité du système en question (volume des transactions supportables, nombre d'utilisateurs, caractère centralisé ou décentralisé, le nombre d'interfaces et de modules,...),
- l'âge des applications,
- les changements opérés au personnel chargé,
- la profondeur des changements opérés aux applications (profonds ou superficiels),
- le niveau ou degré d'intervention manuelle dans le système et son degré d'intégration

## **B. Questionnaire d'évaluation du risque inhérent**

A la suite de ces généralités sur le risque inhérent lié à l'activité de e-commerce d'un site, il est évident que toute tentative de modélisation ou de standardisation du processus d'évaluation du risque inhérent est à proscrire. Des facteurs ou des considérations peuvent, en effet, être omises ou insérées indûment et la complexité des risques n'est pas de nature à être domptée par des check-lists ou des questionnaires d'évaluation.

Cependant, nous allons présenter un questionnaire indicatif pouvant aider à évaluer le risque inhérent, au niveau général et spécifique. L'objectif n'est nullement d'être exhaustif ni de proposer une solution ; il s'agit juste de donner une méthode ou une façon d'aborder cette évaluation et de permettre une quantification, même subjective, du risque par rapport à une

échelle déterminée selon le jugement professionnel de l'expert comptable. Des variables clés influant sur le niveau du risque inhérent sont donc évaluées sur une échelle de risque allant de 1 (faible) à 5 (élevé), et puis multipliées par un coefficient de signification allant de 1 (faible importance) à 10 (importance cruciale). Le score final obtenu permet de situer le risque inhérent du site dans un intervalle de risque inhérent élevé ou modéré ou faible.

<b>Variables / questions clés</b>	<b>Valeur descriptive</b> 1 (très faible) à 5 (très élevé)	<b>score</b>	<b>Coef. de signification</b> (de 1 à 10)	<b>Valeur pondérée</b>
<i>Facteurs de risque inhérent généraux :</i>				
Intégrité de la direction du site	. Direction très intègre et honnête . Direction sérieuse et rigoureuse . Direction ayant commis certains actes malveillants . Direction peu scrupuleuse ou peu intègre	1 2 3 à 4 4 à 5	10	30
Compétence de la direction du site	. Direction très compétente et expérimentée . Certains responsables clés sont assez compétents . Les personnes clés ne sont pas suffisamment comp. . Direction sans expérience ni compétence prouvée	1 2 3 à 4 4 à 5	10	30
Comportement et coopération avec l'équipe d'assurance	. Direction très disponible et coopérante . Direction donnant de l'égard à la mission . Direction occupée par d'autres tâches . Direction réticente et peu collaboratrice . Direction entravant ou empêchant la mission	1 2 3 4 5	8	24
Stabilité de la direction	. Direction très stable, soudée et synergique . Direction stable mais peu soudée . Direction autocratique dépendant d'une seule tête . Grands mouvements de rotation et démission	1 2 3 à 4 4 à 5	5	10
Stabilité de l'environnement légal, fiscal ou réglementaire	. Absence de lois ou règlements concernant le site . L'environnement légal ou fiscal et stable . Variations mineures de l'environnement juridique . Nouveaux textes ou règlements applicables au site . Le site est soumis à des lois strictes et surveillées	1 2 3 4 5	8	16
Conjoncture économique du site ou de l'activité	. Le site est une activité secondaire de l'entité . Le site subit la concurrence d'autres noms . Le site est l'activité principale de l'entité . Les produits ou la technologie sont sujettes à l'obsolescence . L'entité a des problèmes de continuité d'exploitation	1 2 3 4 5	7	7
Type d'activité sur le site Web	. Site informationnel (orienté public) . Site informationnel (orienté client) . Site de distribution (sans paiement) . Site de distribution (avec paiement) . Site transactionnel (orienté B to B)	1 2 3 4 5	9	27
Variation de l'activité, structure ou pratiques du site	. Le site est récent (pas de période de référence) . Le site a connu peu de variations en ventes/visite . Le site a connu des variations de visites . Le site a enregistré des variations de transactions . Le site a connu des variations de structure/pratiques	1 2 3 4 5	6	18
Audience et fréquentation du site	. Site peu visité . Site visité avec faible période de navigations . Site bien fréquenté et référencé . Site très fréquenté et très notoire	1 2 3 à 4 4 à 5	9	27
Conclusions des précédentes missions d'assurance	. Vérification récente : sans faiblesses . Vérification récente : faiblesses non significatives . Vérification non récente : quelques faiblesses . Vérification non récente : faiblesses significatives . Pas de mission d'assurance (ou audit informatique)	1 2 3 4 5	7	35

<b>Variables / questions clés</b>	<b>Valeur descriptive</b> 1 (très faible) à 5 (très élevé)	<b>score</b>	<b>Coef. de signification</b> (de 1 à 10)	<b>Valeur pondérée</b>
<i>Facteurs spécifiques de risque inhérent</i>				
Période depuis la dernière revue du système	Un score de 5 indique 5 ans ou plus ou jamais Un score de 4 équivaut à 4 ans etc.	1 à 5	4	20
Importance du site (en volume, budget du projet, revenus)	. Revenu < 100 KTND / budget < 50 KTND . Revenu entre 100 KTND et 300 KTND / budget entre 50 KTND à 200 KTND . Revenu > 300 KTND / budget > 200 KTND	1 2 à 3 4 à 5	4	8
Caractère de l'activité du site	. Système local . Branche ou unité d'affaire . Activité principale de l'entité	1 2 à 3 4 à 5	8	16
Etendue du système	. Partie d'un département . Département entier . Multi-départements . Toute l'organisation . Organisation et externe	1 2 3 4 5	4	16
Effet d'une panne du système	. Pas d'effet immédiat . Perturbations aux utilisateurs . Perte d'image . Perte de revenus . Perte d'affaires, revenus et image	1 2 3 4 5	6	24
Exposition aux risques financiers	. Aucune . faible (<10 KTND) . Moyenne (entre 10 à 50 KTND) . Elevée (entre 50 KTND et 200 KTND) . Très élevée (> 200 KTND)	1 2 3 4 5	6	18
Complexité du système de e-commerce	Considérer le nombre d'utilisateurs, système centralisé ou décentralisé, nombre d'interfaces, modules... . Simple . Moyennement complexe . Très complexe	1 2 à 3 4 à 5	8	24
Nombre de personnel travaillant sur le système	. Très petit < 2 . Petit : entre 2 à 6 . Moyen : entre 7 à 12 . Large : entre 13 à 20 . Très grand > 20	1 2 3 4 5	4	8
Nombre d'applications dans le système (ou programmes)	. Une seule . Moins de 4 . de 4 à 10 . de 11 à 20 . Plus de 20	1 2 3 4 5	3	6
Nombre d'utilisateurs du système	. Inférieur à 5 . Entre 5 à 10 . Entre 10 à 20 . Entre 20 à 50 . Supérieur à 50	1 2 3 4 5	4	8
Age des applications	. Plus de 10 ans . de 7 à 10 ans . de 4 à 6 ans . de 1 à 3 ans . Très récentes	1 2 3 4 5	3	15

<b>Variables / questions clés</b>	<b>Valeur descriptive</b> 1 (très faible) à 5 (très élevé)	<b>score</b>	<b>Coef. de signification</b> (de 1 à 10)	<b>Valeur pondérée</b>
Etendue des changements au système, procédures ou processus	Considérer pour la ré-ingénierie du système : . Changements superficiels . Moyennes modifications . Modifications majeures	1 2 à 3 4 à 5	8	8
Nature des procédures de changement	. Procédures d'entreprise . Procédures locales . Pas de procédures	1 2 à 3 4 à 5	8	8
Méthodologie de développement du système	. Système est acquis et non développé en interne . Méthodologie standardisée avec documentation des procédures et standards . Méthodologie standardisée sans documentation des procédures et standards . Pas de méthodologie standardisée mais une équipe de développement expérimentée . Méthodologie expérimentale . Pas de méthodologie de développement ni de documentation	0 1 2 3 4 5	5	0
Sous-traitance lors du développement	. Système est acquis et non développé en interne . Petite quantité, un seul fournisseur . Petite quantité, plusieurs fournisseurs . Importante quantité, un seul fournisseur . Importante quantité, plusieurs fournisseurs . 100% sous-traités	0 1 2 3 4 5	2	0
Plateforme de développement	. Système est acquis et non développé en interne . Largement adoptée et utilisée . Nouvelle mais généralement acceptée . Nouvelle et peu adoptée . Inconnue	0 1 2 3 à 4 4 à 5	2	0
Durée de développement	. Système est acquis et non développé en interne . Moins de 3 mois . 3 à 6 mois . 6 à 12 mois . 12 à 18 mois . Plus de 18 mois	0 1 2 3 4 5	2	0
Nature du pack logiciel acquis	. Système développé en interne et non acquis . Solution commerciale largement adoptée . Solution sur mesure, maintenance par constructeur . Développé par le vendeur, maintenu en interne . Développé conjointement, maintenu par vendeur . Développé conjointement, maintenu en interne	0 1 2 3 4 5	2	2
Sélection de la solution	. Système développé en interne et non acquis . Parmi plusieurs candidats selon cahier de charges . Sur devis parmi des constructeurs connus . Sur devis parmi des boîtes locales . Acquis directement auprès d'une boîte réputée . Acquis directement auprès d'une boîte inconnue	0 1 2 3 4 5	2	4
Coût de la solution de e-commerce acquise	. Système développé en interne et non acquis . Faible ou négligeable . Moyen . Importante . Très élevée	0 1 2 3 à 4 4 à 5	2	6

Variables / questions clés	Valeur descriptive	score	Coef. de signification (de 1 à 10)	Valeur pondérée
	1 (très faible) à 5 (très élevé)			
Principes demandés en certification	. Protection des données personnelles	5	6	30
	. Confidentialité	4		
	. Pratiques commerciales et intégrité des opérations	3		
	. Sécurité	2		
	. Accessibilité	1		
. Combinaison de principes : additionner le score de chacune				
<b>TOTAL SCORE :</b>				<b>443</b>

### C. Analyse du risque inhérent à l'activité du site

Grâce à ce questionnaire de scoring, l'expert comptable peut procéder à une évaluation du risque inhérent selon les hypothèses d'importance qu'il accorde à chaque critère contribuant au risque inhérent (coefficients) et son évaluation du risque lié à chaque critère (score). La valeur pondérée score x coefficient donne un score total pour chaque mission. Cette méthode permet une évaluation dans le temps et dans l'espace du risque inhérent, puisqu'elle s'exécute de la même façon pour une même entité d'un mandat à un autre, et qu'elle fait subir à deux entités différentes les mêmes critères d'évaluation.

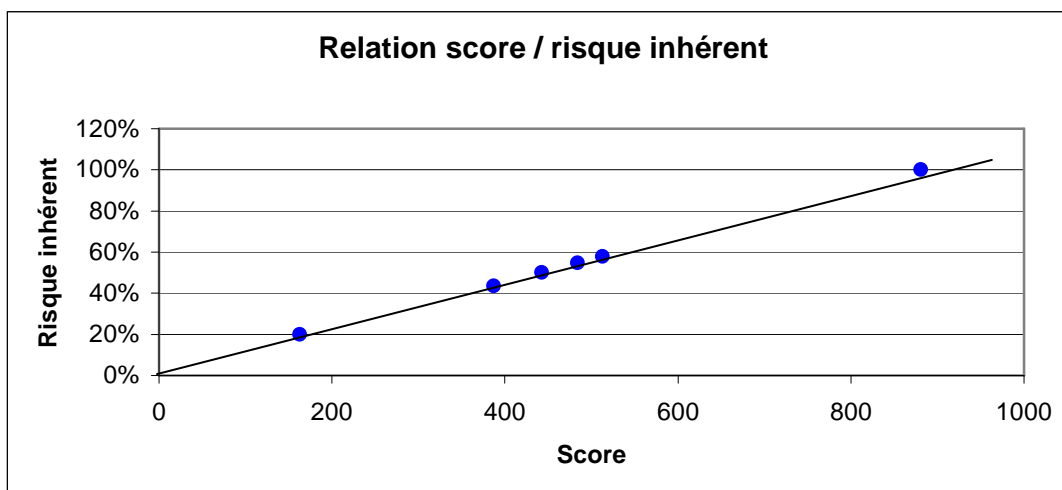
Afin d'exprimer le score total par un pourcentage de risque inhérent, l'expert comptable peut calculer le score minimal, maximal et moyen pouvant être obtenu et alimenter son analyse des fourchettes de risque par les différentes missions qu'il effectue. Ainsi, il peut fixer le niveau limite des scores qui donnent un risque inhérent faible, modéré ou élevé.

Dans notre cas, le score le plus faible pouvant être atteint par une entité est de 163, et le plus élevé est de 881. Le niveau moyen peut se situer aux alentours de 484. Pour le risque le plus faible, l'expert comptable peut affecter un risque inhérent de 20%. En effet, s'agissant du domaine du e-commerce où le risque inhérent est par définition élevé, un site opérant dans des critères de risque jugés faibles est exposé à ce que 20% de ses transactions peuvent contenir des erreurs ou incidents (estimation à la diligence de l'expert comptable).

Dans le but de déterminer la relation entre le score et le risque inhérent, l'expert comptable peut combiner l'ensemble des observations faites durant ses missions afin de calculer la droite qui s'ajuste au plus près à ces observations par la méthode des moindres carrés. Dans notre cas, le tableau suivant récapitule les observations faites pour divers types de missions :

Cas	1	2	3	4	5	6
Désignation	Min	Site 1	Notre cas	Moy.	Site 2	Max
Score	163	387	443	484	513	881
Risque inhérent	20%	à déterminer	à déterminer	à déterminer	à déterminer	100%

La droite de régression a pour équation :  $y = ax + b$ , où  $y$  est fonction du score  $x$  obtenu et  $a$  est le coefficient de régression à déterminer. La constante  $b$  doit être égale à 0 car pour un score de 0, le risque inhérent est nul. Cette droite peut être visualisée grâce au graphique suivant, où les points en bleu représentent les différentes observations de cas effectués :



Le calcul du coefficient de régression dans notre cas donne  $a = 0,001128$ , soit 0,1128%. Ainsi, le score obtenu pour chaque mission multiplié par 0,1128% donnerait l'évaluation du risque inhérent selon cet exemple. Ce qui donnerait l'évaluation suivante des risques inhérents des différentes observations (le risque inhérent pour notre cas est ainsi de 50%) :

Cas	1	2	3	4	5	6
Désignation	Min	Site 1	Notre cas	Moy	Site 2	Max
Score	163	387	443	484	513	881
Risque inhérent	20%	44%	50%	55%	58%	100%

Rappelons, tout de même, que ce modèle d'évaluation n'est pas un modèle absolu et dénué d'imperfections. Il reste entaché par la subjectivité liée à l'évaluation faite par chaque expert des critères formant le risque inhérent, de l'importance de ces critères, du niveau minimal du risque inhérent ainsi que par les imprécisions dues à la supposition que la relation risque / score est linéaire. Cependant, l'approche probabiliste de l'auditeur est elle-même basée sur plusieurs hypothèses et évaluations subjectives émanant de l'auditeur et générant des imperfections et des imprécisions. Il faut donc insister que ce questionnaire de scoring doit être considéré, non pas comme une méthode absolue, mais comme un outil de travail.

Nabil Ghodhbane  
Expert comptable membre de l'ordre