

Considérations pour l'évaluation du risque de contrôle lié à l'activité du site (Partie 2)

Suite à l'évaluation des composants généraux du système de contrôle interne abordée la semaine dernière, nous proposerons dans ce dossier un guide pour l'évaluation des composants de contrôle interne spécifiques à l'activité d'un site, à savoir ceux liés aux contrôles généraux du système informatique et ceux liés aux sécurités et applications Web soutenant le site.

2. Programme de travail pour l'évaluation des contrôles généraux du système informatique :

Les contrôles généraux du système informatique s'adressent aux opérations et activités des départements chargés de la technologie et des systèmes d'information. Comprendre et évaluer les contrôles généraux du système d'information est une étape cruciale dans l'appréciation des systèmes de contrôle interne appuyés par des technologies d'information et aussi, dans toute approche d'audit financier, d'audit informatique, d'audit interne et de mission d'assurance telle que WebTrust (élaborée par l'AICPA¹ et le CICA²). Les normes internationales d'audit et d'assurance, les standards américains, les organismes chargés du développement des systèmes d'informations, ainsi que la norme WebTrust précitée, font l'unanimité autour de l'importance de l'évaluation des contrôles généraux du système d'information. Ainsi, si les contrôles généraux sont jugés faibles ou faillibles, il en sera de même pour les contrôles d'application, les contrôles sur les infrastructures Web et les contrôles rattachés aux transactions Web de l'entité.

Afin de présenter une démarche pratique pouvant aider l'expert comptable en charge d'une mission rattachée à un site Web, nous avons essayé de synthétiser plusieurs des préconisations d'organismes tels que l'IFAC, le COSO³, le CoBIT⁴ dans un programme de travail. Nous y retrouverons les travaux et vérifications à faire dans les principales composantes des contrôles généraux d'un système informatique telles qu'identifiées par ces organismes :

<i>Programme de travail pour la vérification des composants des contrôles généraux du système informatique</i>	WP REF	Fait par & date
A. Général:		
1. Revoir les constatations et les recommandations des précédents audits ou vérifications et s'assurer que des actions correctives ont été entreprises. Documenter les actions prises pour chaque recommandation et déterminer les constatations ou les recommandations qui n'ont toujours pas été traitées.		
2. Si applicable, revoir les précédents rapports d'audit interne pour le département des technologies d'information. Déterminer si les faiblesses ou les non-conformités relevées ont été considérées comme significatives et ont été résolues.		
3. Examiner les autres rapports de spécialistes externes ou d'agences réglementaires ayant émis des rapports sur le système informatique de l'entité et focaliser sur leurs constatations et leurs recommandations.		
4. Documenter les plateformes informatiques utilisées ou exploitées par l'entité ainsi que les applications exécutées sur chacune des plateformes. Cette documentation doit relever : <ul style="list-style-type: none">• Les modèles des équipements• Les constructeurs• La quantité		

¹ American Institute of Certified Public Accountants

² Canadian Institute of Chartered Accountants

³ Committee of Sponsoring Organizations of the Treadway Commission

⁴ Control Objectives for Business & Related Technology : modèle d'audit des systèmes d'information (© copyright ISACA)

Programme de travail pour la vérification des composants des contrôles généraux du système informatique	WP REF	Fait par & date
<ul style="list-style-type: none"> • Les informations pour les applications logicielles doivent inclure : <ol style="list-style-type: none"> 1. Le nom de l'application et son objet 2. Le vendeur 3. La version du logiciel 		
B. Organisation du département des technologies de l'information (TI)		
1. Obtenir l'organigramme du département chargé du système d'information et évaluer son organisation afin de déterminer si les fonctions clés (programmeurs, analystes, opérateurs, WebMaster, responsable réseau...) sont adéquatement séparées et ne contiennent pas d'incompatibilités		
2. A travers des discussions avec le personnel du département, évaluer la séparation effective des fonctions critiques de traitement.		
3. S'assurer que le département TI est une cellule de support au sein de l'organisation et qu'elle n'est pas habilitée à initier ou autoriser des transactions.		
4. Déterminer s'il y a un comité des TI au sein de l'organisation chargé d'encadrer et de surveiller les activités du département des TI. Obtenir et consulter les procès verbaux de ses réunions.		
C. Environnement et accès physique aux centres informatiques		
Note: L'environnement physique doit être examiné eu égard à la taille des opérations et aux recours à des tiers fournisseurs de services pour les activités de e-commerce.		
1. Evaluer la bonne localisation des centres informatiques dans l'immeuble qui les abritent. S'assurer que les pièces avoisinantes et étages mitoyens ne comportent pas de risques (matériaux inflammables, fortes radiations électromagnétiques, fourneaux ou chaleur excessives...).		
2. Visiter les centres informatiques (incognito et inopinément si possible). Documenter les mesures prises pour contrôler l'accès physique aux locaux tels que le centre des données, la pièce des ordinateurs ou celle des routeurs, hubs et autres moyens de télécommunication : <ul style="list-style-type: none"> • Identifier les portes et les séparations et s'assurer de la restriction des accès, • vérifier que les visiteurs signent des registres permettant de retracer et horodater leurs entrées et sorties. • 		
3. Déterminer si des caméras de surveillance, des gardes ou des clés magnétiques ou électroniques sont utilisés pour restreindre les accès physiques et les surveiller.		
4. S'assurer que les contrôles suivants sur l'environnement physique ont été installés : <ul style="list-style-type: none"> • Equipements anti-incendie (extincteurs, tuyaux de pompiers...), • Onduleurs et systèmes d'alimentation continue • Générateurs de secours • Contrôleurs d'humidité et de température, • Disjoncteurs et interrupteurs d'urgence, • Détecteurs de fumée et d'eau • Eclairage d'urgence S'assurer que ces systèmes sont fonctionnels, régulièrement testés et maintenus (par des contrats de maintenance par exemple)		
5. Vérifier l'existence d'aérateur et de systèmes de climatisation. S'assurer qu'ils sont fonctionnels et bien entretenus et qu'en cas de panne, d'autre solution de conditionnement d'air sont prévues.		
6. Déterminer la localisation des consoles système permettant d'exploiter le système. S'assurer qu'elles sont sises dans les locaux du centre informatique.		
D. Contrôles d'accès et de sécurité		
1. Accès physique:		
S'assurer que l'accès à la pièce des ordinateurs et serveurs est limité à une liste d'opérateurs et leur superviseur. Déterminer si : <ul style="list-style-type: none"> • Des cartes d'identification (ID) électroniques codées ou des clés manuelles sont utilisées pour l'accès 		

Programme de travail pour la vérification des composants des contrôles généraux du système informatique	WP REF	Fait par & date
<ul style="list-style-type: none"> • Des clés de verrouillage des ordinateurs sont utilisées • Une librairie des accès et des privilèges d'utilisation des ordinateurs et des applications est établie • Un journal écrit des accès est tenu et vérifié périodiquement 		
2. Accès logique		
a. Déterminer si une procédure de sécurité des données existe et communiquée au personnel. En obtenir une copie pour la revoir et l'évaluer. S'assurer qu'elle traite des questions cruciales telles que la protection des données, la confidentialité de l'information et l'utilisation de mots de passe.		
b. Déterminer comment les ressources système sont protégées sur l'ordinateur central, les serveurs connexes, les microordinateurs et les ordinateurs clients du réseau. Identifier toutes les applications qui fournissent leurs propres mécanismes de sécurité. c. S'assurer que les contrôles suivants sont installés et fonctionnels : <ul style="list-style-type: none"> • Un identifiant unique (ID) et un mot de passe sont assignés à chaque utilisateur, • Le mot de passe doit avoir une longueur minimale, être une composition de caractère numériques, alphanumériques et spéciaux, combiner des lettres minuscules et majuscules et ne pas figure dans un dictionnaire • Les terminaux inactifs pendant une certaine période (30 minutes en moyenne) sont automatiquement déconnectés, • Les utilisateurs sont contraints de changer de mot passe périodiquement (90 jours au plus), • Les vieux mots de passe ne sont plus utilisables ni consultables, • Les mots de passe sont bien masqués et protégés sur le système. 		
d. Pour les systèmes allouant l'accès à distance moyennant des connexions modem, s'assurer que le système vérifie automatiquement le numéro d'appel et l'utilisateur autorisé et contacte cet utilisateur avant d'autoriser l'accès.		
e. Obtenir et vérifier la liste de tous les utilisateurs, les droits et les privilèges d'accès. S'assurer de sa conformité à l'organisation et de la non existence de fonctions incompatibles.		
f. Documenter les procédures de requête et de suppression d'accès au système. S'assurer qu'une autorisation appropriée est obtenue avant de consentir tout accès. Evaluer les procédures pour éliminer les ID et mots de passe des utilisateurs ayant démissionné ou quitté l'entité.		
g. Sélectionner un certain nombre d'utilisateurs définis dans le périmètre de sécurité du système et vérifier que l'accès au système a été adéquatement autorisé. Les interviewer pour s'assurer de leur compréhension des procédures de sécurité logique.		
h. Sélectionner un certain nombre de serveurs sensibles et s'assurer que tous les accès aux données ou aux applications ont été appropriés.		
i. Identifier les utilisateurs qui ont des accès privilégiés sur le package de sécurité (fichiers de sécurité, fichiers sensibles, ...) et documenter la surveillance de leurs activités.		
j. S'assurer que les derniers correctifs de sécurité des systèmes d'exploitation (tels que Unix ou Windows NT) on été installés.		
k. Déterminer si les événements liés à la sécurité ou les violations aux procédures ont été journalisées et revues par l'administrateur de sécurité du système. Sélectionner un certain nombre de ces événements pour les vérifier en substance et confirmer leur contrôle par cet administrateur.		
E. Développement du système et procédures de changement		
1. Obtenir les procédures relatives au développement du système et les processus de changement des programmes et applications. Comprendre et évaluer ces procédures en vérifiant que les modifications du système sont sujettes aux étapes suivantes : <ul style="list-style-type: none"> • Autorisation adéquate pour installer tout changement dans un programme, • Documentation appropriée décrivant la nature et la logique des changements proposés, • Une méthodologie adéquate d'essai et de décomposition des changements sur un environnement de test, avant leur incorporation au système réel, • Une journalisation de toutes les modifications et les changements opérés au 		

Programme de travail pour la vérification des composants des contrôles généraux du système informatique	WP REF	Fait par & date
système est maintenue		
2. Déterminer si l'organisation a mis en place une méthodologie de développement de nouvelles applications systèmes. S'assurer que cette méthodologie est aussi appliquée pour les systèmes acquis.		
3. Documenter les aspects du SDLC ⁵ effectués par le personnel du département TI en considérant : <ul style="list-style-type: none"> • La participation et la signature des utilisateurs, • Les tests d'approbation, • La revue, l'approbation et la documentation adéquates à la fin des étapes clé du processus de développement 		
4. Sélectionner un certain nombre de systèmes ou d'applications et vérifier la documentation de développement et sa conformité avec la méthodologie SDLC.		
6. Evaluer les procédures de changement pour s'assurer que les contrôles clés suivants existent : <ul style="list-style-type: none"> • Aucun changement ne peut être opéré dans les programmes ou les fichiers avant l'obtention d'une autorisation écrite, • Seuls les programmeurs peuvent effectuer les changements aux programmes, • des demandes de changement des programmes sont établies, • Les utilisateurs approuvent ces demandes de changement, • Les utilisateurs classent périodiquement les demandes de changement selon leur priorité, • Les utilisateurs acceptent les changements en confirment par leurs signatures avant l'installation de ces changements, • Le changement est installé dans l'environnement opérationnel par un personnel différent de celui l'ayant programmé. 		
7. Vérifier l'application de ces procédures à travers un test sur un échantillon de programmes récemment changés.		
8. Tester les changements non autorisés ou non documentés en exécutant une comparaison du programme actuel changé avec le code source.		
9. Déterminer si un environnement d'essai existe sur le système de traitement afin de permettre le développement et le test des changements opérés avant leur installation.		
10. Documenter les procédures de changement d'urgence des programmes. Voir si les changements d'urgence sont migrés à travers des bibliothèques séparées afin de permettre la revue et l'approbation du changement par la direction.		
12. Tester ces procédures de changement d'urgence à travers un échantillon des récents programmes changés d'urgence.		
13. Documenter les procédures permettant d'effectuer des changements de taux dans les applications (tels que les taux de TVA, remises, marges...)		
14. Déterminer comment la sécurité des bibliothèques de programmes et d'application (contenant les programmes sources et exécutables) est garantie par des logiciels ou autres.		
F. Les contrôles sur le matériel et les logiciels systèmes		
1. S'assurer que les contrôles hardware sur les équipements tels que prévus par le constructeur sont effectués (auto-diagnostics, maintenances régulières, etc.)		
2. S'assurer que le matériel et logiciels acquis sont vérifiés pour éviter toute incompatibilité de fonctionnement ou d'intégration dans le système informatique.		
3. S'assurer que tous les messages d'erreur pouvant survenir dans le système d'exploitation sont identifiés quant à leur fait générateur et leurs mesures de correction.		
4. S'assurer que les supports magnétiques et les autres outils de sauvegarde sont suffisants en capacité et fiables pour la conservation.		
G. Les contrôles sur les traitements informatisés		
1. S'assurer que le personnel affecté aux traitements n'est pas celui assigné au développement. Sinon, déterminer les contrôles alternatifs pour négocier ces		

⁵ SDLC, « Systems Development Life Cycle » ou cycle de vie des développements systèmes : méthodologie de développement

Programme de travail pour la vérification des composants des contrôles généraux du système informatique	WP REF	Fait par & date
incompatibilités.		
2. Vérifier l'existence de tableaux de traitement ventilant les tâches et les responsabilités du traitement et enquêter pour s'assurer qu'ils sont bien assimilés. Observer les utilisateurs lors des traitements.		
3. S'assurer que toutes les données entrantes (saisies ou importées) sont sujettes à des contrôles de validation avant leur traitement.		
4. Vérifier les mouchards afin de s'assurer que les tableaux de traitement sont respectés et que chaque opérateur effectue les traitements qui lui sont assignés sans plus.		
5. S'assurer que les outputs du système sont contrôlés quant à leur exactitude et leur exhaustivité et qu'ils sont transmis aux services ou départements concernés. S'assurer que les outputs sensibles ou confidentiels sont destinés uniquement à des personnes autorisées.		
6. Vérifier que le personnel est formé à faire face à certaines erreurs de traitement et observer qu'il les négocie conformément à ces procédures.		
Sauvegarde et restauration		
1. Revoir les procédures de restauration et de sauvegarde de l'entité. S'assurer que les sauvegardes sont effectuées de façon régulière (par incrémentation par exemple). Examiner le contenu de la sauvegarde et s'assurer que tous les fichiers et programmes sont concernés. S'assurer que le journal des transactions en ligne est sauvegardé pour pouvoir restaurer les transactions ayant mis à jour les bases de données.		
2. Vérifier que les copies de sauvegarde du système, programmes et des fichiers sont transférées à un lieu sûr à intervalle régulier. Vérifier l'inventaire des copies de sauvegarde, sinon effectuer le.		
3. Déterminer si un système de gestion des bandes de sauvegarde existe afin de donner un inventaire des bandes de sauvegarde par location, contenu et date.		
Plan anti-sinistre		
1. Déterminer si un plan de reprise écrit a été développé. Evaluer ce plan à travers son examen et la discussion avec la direction et les principaux responsables. Déterminer si ce plan est mis à jour et inclut les composantes principales des systèmes.		
2. Vérifier si le plan anti-sinistre est testé périodiquement. S'enquérir sur l'étendue des tests ainsi que les rapports de conclusion sur leur déroulement.		
3. Déterminer si les responsables du département TI ont développé un plan de recouvrement des ressources du système d'information. Voir si ce plan inclut le recouvrement des informations dans un site hôte. Vérifier alors le contrat entre l'entité et le fournisseur du site hôte et s'assurer que les conditions, les équipements et les télécommunications au site hôtes sont satisfaisants.		
4. En évaluant le plan anti-sinistre, d'assurer que le recouvrement des applications est effectué selon un ordre de risque croissant (les applications les plus critiques sont recouvrées en premier).		
5. Vérifier si des tests de récupération des informations technologiques ont été effectués au site hôte. Obtenir les résultats et vérifier que les objectifs sont atteints.		

3. Evaluation de la sécurité du serveur et des applications Web de l'entité

Après avoir évalué les contrôles généraux liés au système informatique de l'entité, l'expert comptable procède à l'évaluation de contrôles encore plus spécifiques aux activités de e-commerce, à savoir celle des serveurs et des applications Web utilisées. Cette appréciation, couplée avec celle de contrôles généraux du système informatique, contribuera à mieux évaluer l'existence et l'application de certains contrôles cruciaux et permettra de détecter les faiblesses structurelles, conceptuelles ou opérationnelles qui pourraient influencer le risque d'audit de l'expert comptable dans sa mission.

A travers le programme de travail suivant, nous allons présenter certaines vérifications et indications de travaux pouvant constituer un repère pour évaluer les infrastructures et les applications Web utilisées :

Programme de travail pour la vérification des infrastructure et des applications Web de l'entité	WP REF	Fait par & date
A. Les applications Web		
<p>1. Vérifier que l'affichage des informations inutiles est évité : S'assurer que sources HTML, JavaScript ou autres langages scripts ne contiennent pas des informations pouvant être exploitées par des pirates (tels que le nom des développeurs, les fonctions désactivées, des détails sur les fonctions et paramètres CGI⁶, les outils utilisés). De même, vérifier les messages d'erreur provenant des applications Web pour s'assurer qu'elles ne donnent pas des indications trop détaillées sur l'origine des erreurs.</p>		
<p>2. Vérifier qu'un processus d'accès robuste est installé : Quand les applications Web demandent aux utilisateurs d'accéder en s'authentifiant, vérifier que le processus est désigné de façon à ce que :</p> <ul style="list-style-type: none"> • les messages d'erreurs de connexion ne doivent pas indiquer qui du mot de passe ou de l'ID est erroné, • les verrouillage des comptes pour erreurs successives de connexion, dans un environnement d'authentification basique http, sont interdites afin d'éviter le blocage et les attaques par force brute, • les ressources système ne sont allouées qu'une fois l'authentification et la connexion établies afin d'éviter les attaques pour déni de service et améliorer la disponibilité et l'accessibilité. 		
<p>3. Vérifier que les sessions inactives pendant un certain temps désigné sont fermées, si elles peuvent présenter un risque d'accès aux navigateurs en veille.</p>		
<p>4. S'assurer que l'entité utilise des protocoles de sécurisation des sessions tels que SSL pour chiffrer les sessions entre un navigateur et le serveur Web et éviter toute interception de données (surtout pour les pages ou sessions les plus sensibles)</p>		
<p>5. S'assurer que les opérations GET et POST sont installées avec attention: Vérifier que l'opération POST est préférée à GET pour l'obtention des informations sensibles provenant des utilisateurs (en effet, la fonction GET est enregistrée dans l'historique du navigateur et peut révéler des informations confidentielles du type http://www.site.com/scripts/login.cgi?utilisateur=mohamed&motdepasse=ali)</p>		
<p>6. Vérifier que l'utilisation des champs de formulaires est limitée : s'assurer que les champs HTML cachés ne contiennent pas d'informations ou paramètres sensibles (en effet, même si non affichés sur la page Web, ces champs peuvent être facilement consultés sur le code source HTML).</p>		
<p>7. S'assurer que l'utilisation des cookies est contrôlée avec précaution : Vérifier que les cookies utilisés entre le serveur Web et le navigateur sont paramétrées de telle façon à éviter de contenir toute mentions inutiles ou sensibles. A ce propos, vérifier les paramètres suivants des cookies : Name (identificateur du cookie), Domain et Path (hôte et URL où le navigateur va transmettre le cookie), Expires (quand le cookie ne sera plus gardé par le navigateur), Secure (si le cookie doit être envoyé sur une session sécurisée) et Data (chaîne de caractère du cookie). Vérifier aussi, pour les navigateurs paramétrés de façon stricte à refuser tout envoi ou acceptation de cookie, les incidences sur l'exécution de l'application Web.</p>		
<p>8. S'assurer que les entrées faites par les utilisateurs sont validées: L'application doit vérifier que les données saisies par les utilisateurs et transmises par le navigateur à l'application sur le serveur Web sont plausibles et logiques. S'assurer que l'application détecte et refuse les données qui sortent d'un certain champ, le caractère numérique ou alphanumérique, la plausibilité des dates, l'existence de caractères spéciaux pouvant être mal interprétés par l'application (tels que % ; ' « <% etc.) Vérifier que l'application ne compte pas sur des filtres du côté client (tels que des JavaScripts) car il peuvent être trafiqués par un utilisateur malveillants.</p>		

⁶ CGI, « Common Gateway Interface » : programme exécuté du côté serveur permettant l'affichage de données et de pages dynamiques

Programme de travail pour la vérification des infrastructure et des applications Web de l'entité	WP REF	Fait par & date
<p>9. Vérifier que les scripts sont bien construits :</p> <p>Les scripts CGI sont utilisées par les applications Web pour communiquer avec des ressources telles que les systèmes et les bases de données internes de l'entité et forment une cible privilégiée pour les pirates. C'est pourquoi il faut vérifier les mesures suivantes :</p> <ul style="list-style-type: none"> • Les scripts CGI sont sauvegardés dans un répertoire séparé et singulier du serveur Web (le plus commun est cgi-bin) • Ils ne sont accessibles que par des administrateurs valides et autorisés, • Ces répertoires n'incluent pas des programmes interprète ou de commande (tels que Perl ou command.com), • Les entrées clients aux CGI sont validés avant (voir contrôle n° 8), • L'entité utilise des outils pour vérifier les vulnérabilités dans ses CGI (tels que CGIWrap, TaintPerl, ...) • Vérifier qu'il y a suffisamment de mémoire allouée aux CGI (pour éviter les saturations de la mémoire tampon), • Vérifier qu'il a un journal (ou CGI log) enregistrant tout ce que font les CGI, • S'assurer que les scripts sont écrits par des programmeurs expérimentés. 		
<p>10. S'assurer que la sécurité du serveur, de l'hôte et des applications Web ont été vérifiées avant leur entrée en exploitation:</p> <ul style="list-style-type: none"> • Vérifier que les scripts ont été entièrement testés pour éviter des contenus subversifs • Vérifier que les scripts permettant aux utilisateurs d'envoyer des mails utilisent des programmes mail sécurisés (tels que /usr/lib/sendmail au lieu de /bin/mailx ou /usr/ucb/mail) • Vérifier que l'utilisation des formulaires est évitée pour ne pas donner le champ libre à des appels de scripts cachés. • Vérifier que les scripts sont tenus dans des répertoires d'exécution non accessibles aux utilisateurs Web. • S'assurer de l'existence de contrôles d'accès sur les répertoires Web et les pages et scripts qu'ils contiennent. 		
<p>11. S'assurer de la sécurité de l'architecture des applications:</p> <ul style="list-style-type: none"> • Vérifier que les connections aux bases de données évitent l'utilisation d'identifiants à privilèges étendus. • Vérifier si le serveur Web est physiquement différent du serveur d'application en queue de file • Vérifier que les données sensibles des consommateurs (telles que les n° de cartes de crédit...) sont systématiquement et efficacement cryptées. 		
<p>B. Logiciel du serveur Web (Logiciels commerciaux de Microsoft ou Sun ou Open Source tel qu'Apache)</p>		
<p>1. Qu'ils soient des logiciels commerciaux (Microsoft ou Sun) ou Open source (Apache), vérifié que ces logiciels ne permettent pas de révéler directement ou indirectement des informations pouvant être exploités par des pirates. Ceci inclut la suppression des références ou la version du serveur, la non possibilité d'indexer les répertoires exécutables afin de ne pas révéler des fichiers cachés, la non possibilité de voir le code source des fichiers exécutables sur le serveur, le non affichage d'informations sensibles sur les certificats, ...</p>		
<p>2. S'assurer que le filtrage de paquets existe et interdit l'accès à des ports alternatifs exécutant des pages sensibles.</p>		
<p>3. Vérifier que toute information sensible est déménagée du serveur Web accessible au public.</p>		
<p>4. Vérifier que les pages sensibles sont protégées par des mots de passe ou des listes d'accès.</p>		
<p>5. S'enquérir sur les bugs connus du type de serveur utilisé et voir si les patchs correctifs préconisés par les constructeurs ont été installés. S'assurer que l'entité est abonnée à des sites ou des newsgroups permettant de la notifier sur toute nouvelle vulnérabilité connue.</p>		

Programme de travail pour la vérification des infrastructures et des applications Web de l'entité	WP REF	Fait par & date
6. S'assurer que les utilisateurs sont adéquatement authentifiés selon le niveau d'authentification requis par le site ou la page Web visité (ceci va de l'authentification basique par des ID et des mots de passes, l'authentification par un challenge/réponse, l'utilisation de certificats ou l'authentification par des token utilisant des mots de passe à usage unique).		
7. S'assurer que les services FTP sont installés avec précaution : Vérifier que les services FTP ne permettent pas aux utilisateurs de charger des fichiers sur le même hôte que le serveur Web pour éviter que des programmes arbitraires ne soient transférés. Si l'entité offre un service FTP, vérifier que les aspects suivants sont respectés sur le serveur : <ul style="list-style-type: none"> • L'utilisation de contrôles d'accès pour placer des limites strictes sur les répertoires et fichiers accessibles via le FTP, • L'utilisation de techniques fortes d'authentification (telles que les certificats basés sur le SSL) pour les opérations FTP PUT. • Ne permettre les accès PUT que sur des sessions serveurs séparées, exécutées sous des identifiants utilisateurs séparés qui ne peuvent être lus par personne (L'identifiant utilisateur pour un accès normal ne doit pas avoir un accès écriture sur les fichiers de documents). 		
8. Vérifier la journalisation des accès aux pages Web (logging) et s'assurer de la revue permanente des journaux (ou logs)		
C. Plateforme Web (Les principales plateformes sont Windows (NT) et Unix)		
1. Vérifier la suffisance des ressources matérielles utilisées : Effectuer un exercice de planification de la capacité pour s'assurer que le CPU, la mémoire et les ressources en disques durs et autres dans la plateforme Web sont suffisantes pour l'usage attendu. Surveiller aussi, en temps réel, l'usage réel de ses ressources systèmes et observer les moments de pics afin de déterminer les éventuelles mises à jour et améliorations à effectuer d'avance avant toute dégradation de performances.		
2. Vérifier les capacités de récupération de la plateforme matérielle en s'assurant qu'elle est fiable et bien testée par rapport aux niveaux de disponibilité requis. Vérifier par exemple l'existence de ressources de secours (alimentation électrique, unités centrales, lecteurs de disques, voire système entier dans un local alternatif et en mode d'attente).		
3. S'assurer que les serveurs Web sont situés dans un local aménagé et dans un environnement sécurisé pour les protéger des menaces (feu, accidents, dommages, vandalisme...)		
4. Vérifier la bonne configuration du système d'exploitation: Les aspects suivants de la configuration du système d'exploitation doivent être vérifiés : <ul style="list-style-type: none"> • Les comptes d'utilisateurs, autres que ceux du serveur Web, Webmaster et les administrateurs autorisés sont supprimés, • Des répertoires racines différents pour le serveur Web et les documents Web sont utilisés, • Les logiciels interpréteurs, compilateur, les Shells et les fichiers de configuration doivent être placés en dehors du répertoire du serveur Web, • Un set minimal d'applications client est installé. • Si un navigateur doit être installé, alors il faut désactiver le téléchargement des contenus actifs (tels que ActiveX et Java), • Si les circonstances l'exigent, alors il faut exécuter des sessions Web différents, sous différents identifiants, pour fournir des types d'accès différents à des utilisateurs différents • L'utilisation du filtrage de paquets (TCP wrappers) pour restreindre les connexions à partir d'hôtes ou services connus et pour journaliser les différentes requêtes de services, • Les fichiers sensibles sont protégés d'accès à travers le Web (mots de passe, fichiers de données sensibles...); 		

Programme de travail pour la vérification des infrastructures et des applications Web de l'entité	WP REF	Fait par & date
<p>5. a. Dans une plateforme « Unix », vérifier les aspects sécuritaires suivants :</p> <ul style="list-style-type: none"> • S'assurer que « chroot » est utilisé sur la racine du serveur Web pour éviter à ce dernier de ne voir aucune partie du fichier système normal, • S'assurer que le serveur Web est démarré en utilisateur racine (pour ouvrir les ports standards http et https : 80/443) puis changé à une autre identifiant utilisateur avec un minimum de privilèges, • S'assurer que les comptes par défaut (tels que lpd et sync) sont supprimés et que les autres comptes privilégiés sont minimisés, • Vérifier que les compilateurs et les scripts setuid/setgid sont supprimés, • Vérifier que le routeur par défaut est configuré comme routeur d'accès, • Vérifier que les services non explicitement requis sont désactivés (exemple : NFS, NIS, les services basés sur RPC, les services de booting, les services basés sur 'r' commandes, UUCP...), • S'assurer que les services 'kernel' et ceux pouvant permettre le 'sniffing' (tels que 'tcpdump') sont désactivés, • En général, consulter le guide d'audit « Unix » pour plus de détails de vérification sur les systèmes « Unix » 		
<p>5. b. Dans une plateforme « NT », vérifier les aspects sécuritaires suivants :</p> <ul style="list-style-type: none"> • S'assurer que seul NTFS est utilisé (Système de fichier NT), • Vérifier que le serveur et la station de travail sont désactivés sur la plateforme NT hôte, • S'assurer que le serveur n'est pas configuré comme un contrôleur de domaine afin d'empêcher les pirates ayant compromis la sécurité du serveur Web d'atteindre un niveau d'accès au domaine, • Vérifier que le serveur Web ne fonctionne pas comme un système, • Vérifier que le compte d'administrateur est renommé de façon obscure afin d'obliger les pirates à le deviner, • S'assurer que les comptes d'invité et les autres comptes d'utilisateurs sont désactivés, • S'assurer que tous les services réseau non requis ou pas nécessaires sont désactivés, • S'assurer que tout rattachement du NetBIOS au TCP/IP est supprimé, • En général, consulter le guide d'audit « NT » pour plus de détails de vérification sur les systèmes « NT » 		
<p>6. S'assurer que de la robustesse des pratiques en matière d'administration du serveur :</p> <ul style="list-style-type: none"> • Vérifier que la connexion de l'administrateur se fait directement de la console centrale. Sinon, s'assurer que la connexion à distance de l'administrateur est basé sur des techniques d'authentification fortes (mot de passe à usage unique, challenge/réponse...), • Vérifier que les connexions administrateur, les échecs, les changements dans la configuration de sécurité et les redémarrages ou arrêts du serveur sont journalisés, • Voir si l'entité utilise des outils tels que 'SSH' pour crypter les sessions administrateur et prévenir des mots de passe administrateur d'être révélés. 		
<p>D. Environnement réseau (Le serveur Web a besoin d'une connectivité, non seulement avec Internet, mais aussi avec l'Intranet. La sécurité de ces réseaux ne touche pas uniquement le serveur et les applications Web mais aussi toute l'infrastructure TI de l'entité)</p>		
<p>1. Vérifier si l'entité a bien estimé ses besoins en bande passante : Opérer une estimation minutieuse de la bande passante et surveiller son utilisation de façon régulière afin d'éviter tout sur chargement, dépassement, ralentissement ou indisponibilité.</p>		
<p>2. Vérifier, pour les systèmes à grands besoins de disponibilité, que des connexions Internet séparées sont maintenues à travers un différent FSI.</p>		

Programme de travail pour la vérification des infrastructures et des applications Web de l'entité	WP REF	Fait par & date
<p>3. S'assurer que les services réseau sont restreints :</p> <ul style="list-style-type: none"> • S'assurer que les services autorisés entre le serveur Web et le réseau interne sont limités à ceux justifiés par des besoins spécifiques et légitimes, • S'assurer que le serveur Web ne prend pas l'initiative d'initier des connexions réseau mais seulement de recevoir et répondre aux requêtes qui lui parviennent, • S'assurer que les connexions au port http 80 (ou https 443 pour SSL), si permises, sont effectués sans activation de l'accusé de réception (le bit ACK contient la valeur NOT) pour éviter le spoofing ou le manque d'accessibilité, 		
<p>4. S'assurer de la bonne configuration du réseau, notamment :</p> <ul style="list-style-type: none"> • Vérifier que le serveur Web est localisé dans un réseau qui ne charrie pas du trafic confidentiel (réseau autonome, Ethernet commuté ou réseau ATM) pour minimiser l'écoute des paquets (sniffing), • S'assurer que le serveur Web est placé dans un emplacement idéal dans l'architecture réseau. Pour ce, considérer les facteurs suivants : <ul style="list-style-type: none"> ▪ Serveur Web sur réseau externe : idéal pour les petites organisations, peu de risques pour le réseau interne, bonnes performances du serveur ; mais peu de possibilités d'intégration et de contrôle, ▪ Serveur Web en dehors du pare-feu : meilleures possibilités de contrôle et peu de risque sur le réseau interne ; mais peu de protection par le pare-feu et coûts de communication élevés, ▪ Serveur Web à l'intérieur du pare-feu : bonnes protection du serveur et possibilités d'intégration ; mais élévation de a complexité du paramétrage et des coûts de la structure, ▪ Serveur Web sur le réseau interne : idéal pour les Intranets, avec une bonne protection par le pare-feu ; mais également des risques sur le réseau interne surtout par les utilisateurs internes. 		
E. Configuration du pare-feu		
<p>1. Etudier les procédures de sécurité et d'environnement du pare-feu, notamment la sécurité physique de l'emplacement du pare-feu et sécurisé, les connexions au pare-feu sont adéquats, les chemins alternatifs d'accès au pare-feu sont désactivés et les procédures de sécurité fournissent les lignes directrices pour la configuration du pare-feu et l'accès à Internet.</p>		
<p>2. S'assurer que l'accès logique au pare-feu est sécurisé et contrôle notamment en limitant le nombre de tentatives, en désactivant les connexions inactives, en utilisant des mots de passe fiables et en journalisant les accès et les tentatives d'accès.</p>		
<p>3. Vérifier la configuration du pare-feu et s'assurer que le système d'exploitation a été endurci</p>		
<p>4. S'assurer que le pare-feu filtre les applications inutiles ou non nécessaires et contrôle les comptes de services et les configurations de scripts sensibles.</p>		
<p>5. S'assurer que la base des règles du pare-feu est conforme avec les lignes directrices de sécurité et fournissent le niveau requis de sécurité.</p>		
<p>6. Vérifier que les paramètres du pare-feu permettent de bloquer les attaques connues (de type Syn flooding, Denial of Service, buffer overflow)</p>		
<p>7. Déterminer si le pare-feu effectue des vérifications d'intégrité du système et consulter les outils de surveillance utilisés par le pare-feu.</p>		
<p>8. Déterminer si outils de détection d'intrusion sont installés dans les points de concentration logique du réseau pour scruter l'état du trafic.</p>		
<p>9. Déterminer comment les points de contrôle du pare-feu permettent de prévenir des attaques Java et ActiveX.</p>		

Programme de travail pour la vérification des infrastructure et des applications Web de l'entité	WP REF	Fait par & date
10. S'assurer qu'il n'y a pas de ports ouverts sur le pare-feu et que les ports administratifs 256, 257 et 258 sont désactivés. Déterminer si des scans de ports sont effectués pour détecter les ports accessibles.		
11. Identifier les protections anti-virus installées pour protéger le pare-feu, le Web et les serveurs emails des virus. Vérifier que les outils antivirus sont opérationnels et actualisés.		
12. Effectuer des tests d'accès à partir des ressources dans la zone démilitarisée (entre le réseau interne et Internet) vers le réseau interne. De même, effectuer des tests d'accès à partir d'Internet vers les ressources situées dans la zone démilitarisée.		
13. Identifier toutes les ressources à l'intérieur de la zone démilitarisée et évaluer leur caractère approprié. Chercher en particulier les applications ou les informations sensibles situées dans cette zone.		
14. Déterminer le type de trafic (http, smtp,...) qui parvient à atteindre la zone démilitarisée et s'assurer qu'il est autorisé.		
<p>F. Pratiques de gestion du réseau, des serveurs et des applications Web (Au-delà des considérations techniques, la sécurité de l'infrastructure Web dépend des pratiques de la direction en matière de planification et de surveillance de la capacité, maintenance et surveillance de la sécurité, gestion des changements, journalisation des événements, détection des intrusions et gestion des incidents)</p>		
<p>1. Pour la planification et la surveillance de la capacité, s'assurer que :</p> <ul style="list-style-type: none"> • Les plateformes matérielles et les réseaux de communication sont calibrés pour supporter toute demande additionnelle sans grands changements dans l'architecture des systèmes, • - Un processus de surveillance de la capacité et de la bande passante du réseau est opérationnel afin d'anticiper tout problème de surcapacité. 		
<p>2. Pour la maintenance et surveillance de la capacité, vérifier que :</p> <ul style="list-style-type: none"> • L'entité souscrit aux sources d'informations avisant des nouvelles technologiques et sécuritaires (mailing lists, sites des fournisseurs d'application ou systèmes, sites sécuritaires, patches et outils de réparation des trous sécuritaires, etc), • L'entité effectue périodiquement une revue de base de sa politique et de ses installations sécuritaires, • L'entité effectue des tests de pénétration et des simulations d'attaques et évalue son infrastructure Web par rapport aux nouvelles menaces apparues. 		
<p>3. Pour la gestion des changements dans le matériel, les logiciels ou le contenu Web :</p> <ul style="list-style-type: none"> - S'assurer que le processus de changement est documenté et clairement assimilé, - S'assurer que l'entité évalue l'impact des changements sur la sécurité de son infrastructure, - S'assurer que les changements sont toujours approuvés et enregistrés de façon claire, - Lors des changements de contenu, s'assurer que tous les liens sont fonctionnels et renvoient à des pages existantes et que les liens rompus sont identifiés et corrigés, - S'assurer que des plans de secours sont prévus avec tout changement opéré. 		
<p>4. Pour le contrôle de la journalisation des événements, s'assurer que :</p> <ul style="list-style-type: none"> • L'entité a développé une procédure de préservation des journaux d'audit et d'événements (sauvegarde des logs, surveillance de la capacité des fichiers logs...), • Les fichiers logs contiennent toutes les informations pertinentes et nécessaires pour surveiller les événements (connexions et échecs, redémarrages et fermetures du système, changements sécuritaires, accès et refus d'accès aux fichiers et objets, surveillance de l'utilisation des systèmes, accès inhabituels, succès et messages d'erreur du pare-feu, tentative d'accès forcé, accès à des ports inhabituels ou non prévus...) 		

Programme de travail pour la vérification des infrastructures et des applications Web de l'entité	WP REF	Fait par & date
<p>5. Pour la détection des intrusions, vérifier qu'un processus de détection des intrusions et utilisé par l'entité, notamment en s'assurant que :</p> <ul style="list-style-type: none"> • Un outil commercial renommé est exploité et constamment actualisé, • Des examens de routine sont effectués par le système pour vérifier son intégrité, • Des tests de pénétration sont effectués manuellement par l'entité pour juger de la vulnérabilité du système, <p>NB : Se baser sur la procédure d'audit n° 8 : « Security assessment – Penetration testing and vulnerability analysis » de l'ISACA⁷ pour effectuer des tests de pénétration et évaluer la vulnérabilité des systèmes.</p>		
<p>6. Pour la gestion des incidents, s'assurer que l'entité est pourvue d'un processus de gestion des incidents qui contient les étapes suivantes :</p> <ul style="list-style-type: none"> • Préparation d'un plan de réponse au incidents et identification des outils, personnel et ressources internes et externes à utiliser en cas d'incident, • Réaction par la détection, l'évaluation de la sévérité de l'incident et la mise en exécution du plan, • Réponse par la mobilisation des ressources disponibles pour traiter l'incident et collecter les informations nécessaires pour le faire, • Contenir les dommages et les répercussions de l'incident soit en éliminant leurs causes soient en réduisant leur impacts, • Restauration du système (à partir des sauvegardes s'il le faut) et vérification que les failles et les vulnérabilités ont été supprimées, • Suivi et revue des contrôles à la lumière des événements rencontrés au cours de l'incident afin de corriger le plan, ajuster les contrôles et doser les ressources futures. 		

A l'issue de ces questionnaires et programmes de travail, l'expert comptable aura effectué une évaluation du système de contrôle interne dans son environnement général, puis au niveau des contrôle généraux du système informatique et, enfin, au niveau des sécurités et applications Web du site. C'est un véritable processus de filtrage des risques qui aboutirait à évaluer le risque liés aux transactions Web faites sur le site. Nous aborderons cet aspect dans la troisième partie de ce dossier que nous présenterons la semaine prochaine.

Nabil Ghodhbane
Expert comptable

⁷ ISACA, "Information Systems Audit and Control Association"