PECB

Réaliser par

Rharif Anass

IRIC2

APPROUVE PAR

Ph.D Yassine

Formation Certified ISO/IEC 27001
Lead Implementer

Exercice 1 : Raisons d'adopter ISO/IEC 27001

Veuillez lire la partie suivante de l'étude de cas fournie pour ce cours :

- Introduction et historique

En vous basant sur ces informations, déterminez et expliquez les trois plus grands avantages de la mise en œuvre de la norme ISO/IEC 27001 pour cet organisme et comment on pourrait mesurer ces avantages grâce aux métriques.

Avantage 1) **Amélioration de la sécurité de l'information**

Comment l'organisme peut-il mesurer cet avantage ?

Amélioration générale de l'efficacité de la sécurité de l'information par exemple la gestion incident. Meilleure sensibilisation a la sécurité de l'information. Revue indépendante du système de management de la sécurité de l'information. Diminution des risques et augmentation de l'imputabilité de la direction.

Avantage 2) **Marketing**

Comment l'organisme peut-il mesurer cet avantage ?

Satisfaction des exigences du client et des autres parties intéressées, Consolidation de la confiance de la clientèle, des fournisseurs et des partenaires de l'organisation. Procurant a l'organisation un avantage concurrentiel.

Avantage 3) **Bonne gouvernance**

Comment l'organisme peut-il mesurer cet avantage ?

Augmentation de l'imputabilité de la direction quant à la sécurité de l'information. Sensibilation et responsabilisation du personnel. Diminution des risques de poursuites judiciaires contre les dirigeants en vertu des principes de due care et de due diligence. Opportunité d'identifier les faiblesses du SMSI et d'y apporter des corrections.

Exercice 2 : Classification des mesures de sécurité

Pour chacune des cinq mesures suivantes, indiquez si elle est utilisée comme mesure préventive, corrective et/ou de détection ; précisez si la mesure est une mesure administrative, technique, managériale ou légale. Justifiez votre réponse.

Exemple : L'installation d'une clôture autour du site de l'organisme.

C'est une mesure préventive qui aidera à sécuriser le site de l'organisme contre l'accès physique non autorisé. L'installation d'une clôture métallique est une mesure technique qui implique une installation matérielle.

1. Attribution des responsabilités en matière de sécurité de l'information à chaque membre de l'organisme

C'est une **mesure préventive** qui Contrôler les opérations par attribue des responsabilités de sécurité a chaque membre. **Mesure administrative** car en a la séparation des taches, c'est une mesure liée à la structure organisationnelle.

2. Mise en place d'un système d'alarme incendie

Mesures de détection car il recherche et identifie les incidents et les problèmes c'est un système d'alarme incendie qui détectent et rapportent la possibilité d'une erreur. **Mesure technique** car cette mesure liée a l'utilisation de mesures techniques ou technologiques (système d'alarme incendie).

3. Cryptage des communications électroniques

Mesures préventives car il prévenir une erreur, une omission des actes malveillants et aussi contrôler les opérations. **Mesures technique**, mesure liée a l'utilisation de mesures techniques ...

4. Enquête sur un incident de sécurité

Mesures correctives car en essayer d'identifier les causes du problème (forencics). **Mesure managériale** car c'est une mesure liée à les revues de direction et les audits.

5. Identification de la législation applicable

Mesures de préventives : publication d'un politique de sécurité de l'information **Mesures légale** c'est une mesure liée aux applications d'une législation aux exigences règlementaires.

Exercice 3 : Établir le contexte de management du SMSI

Fiers du taux de croissance rapide de leurs activités, les dirigeants de Scientia Online Library sont soudainement préoccupés par les aspects de contrôle et de sécurité, surtout depuis qu'il y a eu quelques incidents de sécurité dernièrement. Parce qu'ils vous connaissent bien et qu'ils connaissent votre expertise en sécurité de l'information, ils vous confient le mandat de les aider dans la mise en place d'un système de management de la sécurité de l'information et dans la préparation à la certification ISO/IEC 27001.

La première étape de votre mandat est d'établir le contexte du management de la sécurité de l'information dans l'organisme. Pour eux, c'est le jargon des spécialistes. Ils veulent que vous proposiez une version qu'ils approuveront plus tard.

Pour y parvenir, identifiez, en vous basant sur les informations contenues dans l'étude de cas, quelles seraient les trois plus importantes sources potentielles d'exigences de conformité pour l'organisme. En outre, identifiez quels seraient les deux actifs informationnels ainsi que les deux processus d'affaires que vous jugez les plus critiques pour l'organisme.

Exigences de conformité 1

Ce qu'il faut prendre en considération pour le SMSI :

- Assurer la protection et la confidentialité des données personnelles de tous les utilisateurs du site SOL, en mettant en place des mesures de sécurité adéquates pour protéger ces données contre les fuites, les piratages et les autres formes de compromission.
- Mettre en place des politiques et des procédures de gestion de la vie privée qui respectent les exigences réglementaires en matière de protection des données personnelles.
- Former le personnel et les partenaires à ces exigences et s'assurer qu'ils comprennent leur rôle dans la protection des données personnelles des utilisateurs.

Exigences de conformité 2

Ce qu'il faut prendre en considération pour le SMSI :

- Normes de sécurité du cloud computing, telles que la norme ISO/IEC 27017. Ce qu'il faut prendre en considération pour le SMSI:
- Assurer que l'infrastructure cloud de SOL est sécurisée et conforme aux normes de sécurité du cloud computing en vigueur, en mettant en place des mesures de sécurité appropriées et en réglementant l'accès aux données et aux ressources informatiques.
- Mettre en place des politiques et des procédures de sécurité du cloud qui respectent les normes de sécurité du cloud computing et s'assurer que le personnel et les partenaires comprennent leur rôle dans la protection de l'infrastructure cloud.

Exigences de conformité 3

Ce qu'il faut prendre en considération pour le SMSI :

- Normes de sécurité de l'information en général, telles que la norme ISO/IEC 27001. Ce qu'il faut prendre en considération pour le SMSI:
- Assurer que le système de management de la sécurité de l'information (SMSI) de SOL est conforme aux normes de sécurité de l'information en général, en mettant en place des mesures de sécurité

Identification des actifs

Actif informationnel 1 : Base de données de données personnelles des utilisateurs du site SOL.

Justification de la valeur : Cet actif est crucial pour le fonctionnement du site SOL, car il contient des informations sur les utilisateurs du site, y compris leur nom, leur adresse e-mail, leur adresse postale, leur numéro de téléphone, leur historique d'achats, etc. Ces informations sont utilisées pour fournir des services personnalisés aux utilisateurs et pour gérer leur compte et leur abonnement. Si cette base de données était compromise ou perdue, cela pourrait causer une perte financière importante pour SOL et affecter gravement la réputation de l'entreprise..

Actif informationnel 2 :

Fichiers de livres et d'articles numériques stockés sur l'infrastructure cloud de SOL.

Justification de la valeur : Ces fichiers sont l'actif principal de SOL, car ils sont ce que les utilisateurs achètent et téléchargent sur le site. Si ces fichiers étaient compromis ou perdus, cela pourrait causer une perte financière importante pour SOL et affecter gravement la réputation de l'entreprise. De plus, l'accès à ces fichiers est crucial pour fournir les services aux utilisateurs et pour gérer leur abonnement.

Processus métier 1 : Gestion de la sécurité de l'information

Justification de la valeur : La gestion de la sécurité de l'information est cruciale pour l'organisme, car elle concerne la protection des données sensibles et des actifs de l'organisme, tels que les informations sur les clients, les transactions financières et les données de l'organisme. La bibliothèque en ligne de Scientia Online Library gère de grandes quantités de données et de transactions financières, ce qui la rend vulnérable aux risques de sécurité. En outre, l'organisme a récemment connu des incidents de sécurité, ce qui souligne l'importance de mettre en place un système de gestion de la sécurité de l'information solide.

Processus métier 2 : Gestion de la chaîne d'approvisionnement

Justification de la valeur : La gestion de la chaîne d'approvisionnement est cruciale pour l'organisme, car elle permet de gérer les fournisseurs et les partenaires qui fournissent les livres et autres articles proposés par la bibliothèque en ligne. La croissance rapide de l'organisme a nécessité l'établissement de nombreux partenariats et l'expansion sur le marché international, ce qui implique de nombreux défis logistiques et de gestion de la chaîne d'approvisionnement.

Exercice 4 : Analyse des écarts

En vous référant aux informations fournies dans l'étude de cas sur le fonctionnement du processus de gestion des changements, évaluez le niveau de maturité de ce processus. Également, la direction de l'organisme souhaiterait que vous lui fassiez des recommandations sur l'amélioration des processus actuellement en place afin de mieux se conformer aux exigences de la norme ISO/IEC 27001 sur la gestion des changements.

En se basant sur **Le Modèle CMMI (Capability Maturity Model Integrated), dans le cas de** Scientia Online Library le niveau de maturité de ce processus et le **niveau 4 – Maîtrisé** L'entreprise a institué un processus formel de collecte d'informations pour suivre et gérer le processus, son niveau de performance, son niveau d'atteinte d'objectifs préétablis, son niveau d'efficience (son rapport entre le coût de mise en œuvre et son retour sur investissement). SOL appel la société Web Transit pour résoudre les problèmes avec un contrat de maintenance.

Je suggère pour améliorer un méthodes telle que Le système d'amélioration permanente vérifie et agit sur l'efficacité des processus dans un souci d'efficience. Cette amélioration est intégrée dans le fonctionnement courant de l'entreprise(SOL), et requiert l'engagement et la participation de l'ensemble des collaborateurs. De L'efficacité des processus est revue continuellement, au travers, par exemple d'une revue de processus dans laquelle responsable des services informatiques des processus l'évalue sur la base d'observations, d'indicateurs ou de leur expertise avérée.

Exercice 5 : Définition du périmètre

À partir des informations fournies dans l'étude de cas, indiquez le périmètre du SMSI de l'organisme et déterminez ses limites. La direction souhaite choisir un périmètre qui sera perçu comme ayant une valeur ajoutée pour ses clients et en même temps le délimiter autant que possible pour la certification initiale du SMSI.

Périmètre :

Le périmètre du SMSI (Système de Management de la Sécurité de l'Information) de l'organisme Scientia Online Library (SOL) est la fourniture d'édition et de services d'hébergement Web, ainsi que les services et infrastructures de cloud computing et d'internet.

Définir les limites organisationnelles :

- SOL fournit des services d'édition et d'hébergement Web ainsi que des services et infrastructures de cloud computing et d'internet. Toutes ces activités sont incluses dans le périmètre du SMSI.
- Toutes les activités de l'organisme, qu'elles soient gérées en interne ou externalisées, doivent être prises en compte dans le SMSI. Par exemple, le marketing externalisé doit être inclus dans le périmètre du SMSI si cela a un impact sur la sécurité de l'information.

Définir les limites des systèmes d'information :

- Le SMSI doit couvrir tous les systèmes informatiques utilisés par SOL, qu'ils soient en interne ou hébergés dans le cloud. Cela inclut les serveurs, les ordinateurs, les bases de données, les réseaux et tout autre équipement informatique utilisé dans l'organisme.
- Le SMSI doit également couvrir toutes les applications et les services informatiques utilisés par SOL, tels que les logiciels de gestion de la bibliothèque, les outils de communication et de collaboration, les sites Web et les applications mobiles.

Définir le périmètre physique et les limites :

- Le SMSI doit couvrir les locaux commerciaux de SOL à Phoenix, ainsi que tout autre lieu où sont stockées ou utilisées les données de l'organisme.
- Le SMSI doit également couvrir toutes les données stockées ou transmises sur Internet, y compris celles des partenaires de SOL.

Exercice 6 : Identification des menaces, des vulnérabilités et des impacts

Identifiez au moins deux scénarios de menaces et de vulnérabilités associées aux actifs ci-dessous, et indiquez les impacts potentiels. Précisez également si le risque affecterait la confidentialité, l'intégrité et la disponibilité.

Complétez la matrice des risques et soyez prêt à discuter de vos réponses après l'exercice :

1. Processus de comptabilité
2. Informations personnelles des clients
3. Partenaires

Exercice 6

Actif 1 : Processus de comptabilité						
Scénario de risque	**Menace**	**Vulnérabilité**	**Impacts**	**C**	**I**	**D**
1.	**Divulgation**	**Access non control**	**Impact financier** **Dégradation de la performance** **Interruption du service** **Indisponibilité du service**	**1**	**1**	**1**
2.	**Attaque DDoS**	**Le pare-feu est correctement configuré et dispose d'une bonne atténuation des attaques DDoS FAIBLE**	**Les ressources du site Web seront indisponibles CRITIQUE**	**1**	**2**	**4**

Actif 2 : Informations personnelles des clients						
Scénario de risque	**Menace**	**Vulnérabilité**	**Impacts**	**C**	**I**	**D**
1.	**Vol type: Actions non autorisées**	**Access non control**	**Impacts sur l'image et la réputation Perte de données**	**3**	**1**	**2**
2.	**Virus**	**Antivirus faible**	**Impacts financiers et Atteinte à la vie privée des utilisateurs ou des clients Perte de données Indisponibilité du service**	**1**	**2**	**3**

Actif 3 : Partenaires						
Scénario de risque	**Menace**	**Vulnérabilité**	**Impacts**	**C**	**I**	**D**
1.	**Vol de type: Compromission d'information et Actions non autorisées**	**Pas de coffer-fort**	**Impacts juridiques et réglementaires**	**5**	**2**	**2**

2.	**Interférence humaine accidentelle – suppressions accidentelles de fichiers ÉLEVÉE**	**Les autorisations sont correctement configurées, un logiciel d'audit informatique est en place, des sauvegardes sont réalisées régulièrement FAIBLE**	**Des données critiques seront peut-être perdues,**	**2**	**4**	**2**

Exercice 7 : Options de traitement des risques

À la suite de l'analyse des risques, vous avez identifié que 0,5 % des transactions électroniques (chiffre d'affaires de 10 millions) effectuées par carte de crédit sur le site Web de l'entreprise sont de nature frauduleuse et que 70 % proviennent de transactions dans six pays. La direction de Scientia Online Library veut prendre une décision sur le traitement des risques.

Préparez un résumé leur présentant les quatre options possibles pour traiter ce risque et les actions à entreprendre pour chaque option.

Option 1 :

Mettre en place des mesures de vérification supplémentaires pour les transactions électroniques

Actions à entreprendre :

- Évaluer les différentes options de vérification disponibles, telles que la demande d'informations de vérification de l'identité du client ou l'utilisation de systèmes de détection de fraude avancés.
- Mettre en place les mesures de vérification choisies pour protéger les transactions électroniques contre la fraude.

Option 2 :

Refuser les transactions provenant des pays à haut risque

Actions à entreprendre :

- Mettre en place une politique de refus des transactions électroniques provenant des pays identifiés comme étant à haut risque de fraude.
- Mettre à jour le site Web de l'entreprise pour informer les clients potentiels des restrictions de pays en place.

Option 3 :

Ne rien faire

Actions à entreprendre :

- Continuer à accepter les transactions électroniques sans aucune mesure de protection supplémentaire contre la fraude.

Option 4 :

Augmenter les frais de traitement des transactions électroniques pour couvrir le coût des pertes liées à la fraude

Actions à entreprendre :

- Calculer le coût moyen des pertes liées à la fraude sur les transactions électroniques.
- Déterminer le montant des frais de traitement supplémentaires nécessaires pour couvrir ces pertes.
- Mettre à jour le site Web de l'entreprise pour informer les clients des frais de traitement supplémentaires en place.
-

Exercice 8 : Mesures de sécurité

Pour chacun des articles suivants de la norme ISO/IEC 27001 ou de son Annexe, définissez un plan d'action accompagné d'au moins deux actions concrètes qui permettraient d'assurer la conformité à l'article concerné et de satisfaire aux objectifs.

Exemple : Sécurité du câblage (Mesure A.11.2.3)

- *Utilisation de gaines de câblage réseau pour isoler et protéger de l'interception les communications réseau de l'organisation.*
- *Liste documentée du matériel de câblage autorisé pour éviter l'utilisation de matériel non conforme.*

1. Déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information (Article 7.2 a)

Plan d'action :

- Mettre en place un processus de suivi des compétences de l'ensemble des employés ayant accès aux systèmes de l'organisation.
- Former régulièrement les employés à la sécurité de l'information pour maintenir et développer leurs compétences.

Actions concrètes :

- Établir une liste des compétences requises pour chaque rôle dans l'organisation et vérifier régulièrement que les employés correspondent à ces exigences.

- Organiser des sessions de formation en interne ou externe pour maintenir et développer les compétences des employés en matière de sécurité de l'information.

2. Réagir à la non-conformité (Article 10.1 a)

Plan d'action :

- Mettre en place un processus de gestion des non-conformités qui permette d'identifier et de résoudre rapidement toute non-conformité.
- Former les employés à la détection et à la gestion des non-conformités.

Actions concrètes :

- Établir un processus de signalement des non-conformités, qui permette aux employés de signaler rapidement toute non-conformité.
- Organiser des sessions de formation pour les employés afin de leur apprendre à identifier et à gérer les non-conformités.

3. Dimensionnement (Mesure A.12.1.3)

Plan d'action :

- Mettre en place un processus de dimensionnement des systèmes qui permette de garantir que les ressources informatiques sont suffisantes pour répondre aux besoins de l'organisation.
- Établir un plan de dimensionnement des ressources informatiques qui prenne en compte les besoins futurs de l'organisation.

Actions concrètes :

- Surveiller les performances des systèmes de l'organisation pour détecter tout problème de surcharge ou de sous-utilisation des ressources.
- Établir un plan de dimensionnement des ressources informatiques qui prenne en compte les projections de croissance de l'organisation et qui prévoie l'ajout ou le retrait de ressources en conséquence.

4. Mesures contre les logiciels malveillants (Mesure A.12.2.1)

Plan d'action :

- Mettre en place une politique de gestion des logiciels malveillants qui définisse les mesures à prendre pour protéger l'organisation contre les logiciels malveillants.
- Mettre en place des systèmes de détection et de suppression des logiciels malveillants pour protéger les systèmes de l'organisation.

Actions concrètes :

- Mettre en place un programme de protection antivirus sur tous les ordinateurs de l'organisation et mettre à jour régulièrement les signatures de virus.
- Mettre en place des filtres de messagerie pour bloquer les courriels contenant des pièces jointes dangereuses ou suspectes.

5. Messagerie électronique (Mesure A.13.2.3)

Plan d'action :

- Mettre en place une politique de gestion de la messagerie électronique qui définisse les règles de sécurité à respecter lors de l'utilisation de la messagerie électronique.
- Mettre en place des mesures de sécurité pour protéger la messagerie électronique contre les menaces extérieures.

Actions concrètes :

- Former les employés aux bonnes pratiques de sécurité lors de l'utilisation de la messagerie électronique, telles que la vérification des liens et des pièces jointes avant de les ouvrir.
- Mettre en place des filtres de messagerie pour bloquer les courriels indésirables et les spam.

Exercice 9 : Liste maîtresse des documents

La direction de Scientia Online Library a décidé d'inclure toutes les mesures de sécurité relatives à la gestion de la continuité (mesure A.17) dans son organisme. Pour préparer la mise en œuvre, elle vous demande de compléter la liste maîtresse des documents.

Proposez une liste des documents et des enregistrements qui devraient être générés pour se conformer aux exigences des mesures de sécurité énoncées à la mesure A.17.

Voici une liste de documents et d'enregistrements qui pourraient être générés pour se conformer aux exigences de la mesure A.17 de la norme ISO/IEC 27001 :

- Plan de continuité d'activité (PCA) : document décrivant les mesures à mettre en place pour assurer la continuité des activités de l'organisation en cas de perturbation ou de crise.
- Protocole de crise : document définissant les mesures à prendre en cas de crise pour protéger l'organisation et assurer la continuité de ses activités.
- Plan de reprise après sinistre (PRAS) : document décrivant les mesures à mettre en place pour assurer la reprise des activités de l'organisation après un sinistre.
- Procédure de test du PCA et du PRAS : document décrivant la façon dont le PCA et le PRAS sont testés pour s'assurer de leur fonctionnement correct.
- Enregistrements des tests du PCA et du PRAS : enregistrements des résultats des tests du PCA et du PRAS, y compris tous les écarts constatés et les actions correctives prises.
- Liste de personnel de crise : liste des personnes chargées de gérer la crise et de mettre en œuvre le PCA et le PRAS.
- Plan de communication de crise : document décrivant les moyens de communication utilisés pour informer les parties prenantes en cas de crise.
- Enregistrements des réunions de crise : enregistrements des réunions de crise, y compris les décisions prises et les actions entreprises.

- Liste de fournisseurs de secours : liste des fournisseurs qui peuvent être contactés en cas de crise pour assurer la continuité des activités de l'organisation.

Exercice 10 : Développement d'indicateurs de sécurité de l'information

Pour chacun des articles suivants de la norme ISO/IEC 27001, fournissez deux exemples de métriques qui seraient acceptables pour mesurer la conformité à cet article.

Exemple : Article 5.1 Leadership et engagement

- *Réunions de revue de direction réalisées périodiquement*
- *Taux moyen de participation aux revues de direction à ce jour*

1. Article 10.1 d) Réviser l'efficacité de toute action corrective mise en œuvre

Nombre de non-conformités résolues dans un délai fixé

Pourcentage de non-conformités pour lesquelles une action corrective a été mise en œuvre et qui ont été résolues de manière satisfaisante.

2. Article 5.3 Rôles, responsabilités et autorités au sein de l'organisation

Nombre de fonctions pour lesquelles les rôles et responsabilités ont été clairement définis et communiqués aux employés

Pourcentage de fonctions pour lesquelles les autorisations d'accès ont été correctement configurées et attribuées.

Mesure A.8.1.2 Propriété des actifs

- Pourcentage d'actifs informatiques qui ont été correctement enregistrés et étiquetés
- Pourcentage d'actifs informatiques qui ont été correctement attribués à leur propriétaire légitime

3. Mesure A.8.1.4 Restitution des actifs

Nombre d'actifs informatiques restitués lorsque leur utilisation a été interrompue ou lorsque l'employé a quitté l'organisation

Pourcentage d'actifs informatiques restitués lorsque leur utilisation a été interrompue ou lorsque l'employé a quitté l'organisation.

4. Mesure A.9.3.1 Utilisation d'informations secrètes d'authentification

Nombre de violations de sécurité liées à l'utilisation non autorisée d'informations secrètes d'authentification

Pourcentage de comptes d'utilisateur qui ont été désactivés suite à une utilisation non autorisée d'informations secrètes d'authentification

Exercice 11 : Plan d'actions correctives

Scientia Online Library a été auditée et plusieurs non-conformités ont été identifiées par l'auditeur. Proposez des actions correctives pour chaque non-conformité et justifiez ces actions.

1. Une non-conformité indique que les seuls enregistrements conservés pour le contrôle d'accès des utilisateurs sont ceux relatifs à l'*Active Directory*. Les autres enregistrements ne sont pas conservés.

Cause fondamentale :

Dans ce cas. Les entres enregistrements ne sont pas conserves.

Action corrective :

Utiliser une base des donnes externe pour enregistre les autres enregistrements. Et aussi Vous pouvez utiliser l'audit de sécurité pour suivre diverses activités des utilisateurs sur un ordinateur particulier afin de diagnostiquer et de résoudre les problèmes des utilisateurs légitimes et d'identifier et de traiter les activités illégitimes.

Justification :

Dans la plupart des cas, les tentatives sont légitimes et le réseau doit rendre les données facilement accessibles aux utilisateurs légitimes. Mais dans d'autres cas, les employés, les partenaires et d'autres personnes peuvent essayer d'accéder à des ressources auxquelles ils n'ont aucune raison légitime d'accéder.

2. Une non-conformité indique le manque de formation et d'expérience de l'auditeur interne. Celui-ci n'a pas identifié plusieurs non-conformités qui auraient pu être facilement détectées. En examinant le CV de l'auditeur interne, on a remarqué qu'il avait plus de 20 ans d'expérience en informatique, mais qu'il n'avait jamais suivi un cours d'audit ni jamais effectué d'audit auparavant. Au cours d'un entretien, il a indiqué que cette responsabilité lui avait été confiée parce que personne d'autre ne voulait le faire – il avait bien accueilli ce nouveau défi.

Cause fondamentale :

Dans ce cas l'auditeur interne n'avait jamais suivi un cours d'audit ni jamais n'effectue d'audit auparavant. Alors l'auditeur interne a un manque de formation donc audit n'est pas efficace.

Action corrective :

Auditeur suivre des courses d'audit pour maitrise bien la partie.

Justification :

Formation audit interne qualité : **Maîtriser l'organisation et la réalisation d'un audit qualité** L'audit interne vérifie la pertinence d'un système de management de la qualité mis en place dans une structure (société ou entreprise).

3. Une non-conformité a été soulevée car l'organisme n'a pas traité un incident dans le délai indiqué dans sa politique de gestion des incidents. En effet, la politique de gestion des incidents mentionne explicitement dans ses objectifs que tous les incidents doivent être clôturés dans les cinq jours et que 100 % des incidents doivent se clôturer dans les 15 jours suivant leur première déclaration. Pour cet incident, un client qui a acheté un livre a déclaré avoir été victime d'une fraude par carte de crédit et voulait un remboursement complet. La personne responsable de la gestion de cet incident est tombée malade le lendemain et n'est revenue au travail que 12 jours plus tard. Tant de travail s'était empilé et l'affaire de la fraude par carte de crédit était si complexe que 5 jours ont été nécessaires pour que l'employé puisse s'occuper de cette question, enquêter et clore l'incident. Personne d'autre dans l'entreprise ne s'est occupé des incidents en l'absence de l'employé.

Cause fondamentale :

Dans ce cas la cause fondamentale et ne pas remplacer la personne qui tombe malade la personne responsable de la gestion de cette incidente et aussi le temps de clôtures et petites.

Action corrective :

Augmente le nombre de personnes qui a la responsabilité de gestion des incidents et aussi ajoute 5 jours pour le délai de clôture.

Justification :

Si en augmente le nombre de personnes donc en résoudre plusieurs incidents et aussi augmentation de temps de clôtures donne le temps suffisant de résoudre tous les incidents.

4. Une non-conformité a été soulevée parce qu'au cours de l'audit, le site Web de la compagnie a été mis hors service et que la tierce partie responsable de la maintenance du site n'a pas traité ce problème pendant 72 heures. Personne dans l'organisme ne semblait savoir quoi faire. Le PDG estime que Scientia Online Library a perdu au moins 35 000 $ de revenus au cours de cette indisponibilité, un montant jugé inacceptable pour l'organisme.

Cause fondamentale :

Hors service 72 heures au cour d'audit. Et la tierce partie responsable de la maintenance du site n'a pas traite ce problème.

Action corrective :

Changer la tierce partie responsable de la maintenance par autre, et aussi développer un autre site Web pour l'héberger dans c'est cas.

Justification :

Si on remplace la tierce partie responsable de la maintenance par une autre qui a une bonne expérience comme ça en peut éviter c'est problème et aussi si on a autre site Web on peut diminuer l'argent perdu.

5. Une non-conformité a été soulevée parce que l'auditeur a demandé à un technicien informatique d'effectuer un scan du réseau et plus de 2 000 fichiers musicaux ont été découverts. L'organisme n'interdit pas la copie de fichiers musicaux sur son réseau. L'auditeur a remarqué que certains fichiers musicaux étaient conservés dans des dossiers partagés et que certains employés avaient écouté ou copié plusieurs des chansons d'autres employés. L'auditeur a également trouvé des preuves que certaines des chansons ont été téléchargées à partir de sites Web de partage de fichiers. Lors des entrevues avec des employés sur la question, certains ont mentionné qu'ils avaient copié des chansons de leurs CD personnels afin de pouvoir écouter de la musique pendant qu'ils travaillaient. D'autres ont admis qu'ils avaient téléchargé des chansons à partir de sites Web de partage de fichiers, mais qu'ils n'avaient téléchargé que des chansons dont ils possédaient (et payaient) les CD chez eux – « nous sommes conscients de la politique de l'entreprise en matière de respect des droits de propriété intellectuelle et nous ne pourrions en aucun cas écouter de la musique obtenue illégalement ». Ils ont indiqué avoir procédé de la sorte parce qu'ils souhaitaient écouter certaines de leurs chansons favorites qu'ils possédaient par ailleurs à la maison, mais qu'ils ne voulaient pas apporter leurs CD au bureau et les copier sur leur ordinateur.

Cause fondamentale :

La cause fondamentale et les politiques de l'entreprise.

Action corrective :

Ajoute autre politiques pour interdire des copies des fichiers dans les réseaux, et aussi respecter les donner des autres.

Justification :

Si on ajoute la politique qu'interdire des copies des fichiers dans les réseaux, on garante la **confidentialité**, par exemple on n'a pas des vols des donnes des personne.