PECB

EXERCICES ET DEVOIRS

FORMATION CERTIFIED ISO/IEC 27001 LEAD IMPLEMENTER

Exercice 1 : Raisons de la mise en œuvre d'un SMSI conformément à la norme ISO/IEC 27001

Lisez la section « événements récents » de l'étude de cas et énumérez les principaux avantages que *e-Scooter* peut tirer en mettant en œuvre un système de management de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Devoir 1 : Classification des mesures de sécurité
Pour chacune des mesures de sécurité de l'information suivantes, déterminez leur fonction (préventive, corrective ou détective) et leur type (administrative, technique, managériale ou juridique).

Exemple : Sensibilisation et formation en matière de sécurité de l'information à l'intention des employés de l'organisme
Par fonction, il s'agit d'une mesure préventive qui vise à réduire la probabilité d'incidents de sécurité et à s'assurer que les employés comprennent les risques de sécurité et les pratiques de sécurité. Par type, il s'agit d'une mesure administrative.

1. Séparation des rôles et responsabilités en matière de sécurité de l'information au sein de l'organisme

.....

.....

.....

.....

.....

.....

2. La mise en œuvre du processus de présélection des candidats potentiels avant de se joindre à l'organisme

.....

.....

.....

.....

.....

.....

3. Enregistrement des activités des utilisateurs

.....

.....

.....

.....

.....

.....

4. Enquête sur un incident de sécurité

.....

.....

.....

.....

.....

.....

5. Considérations de la législation applicable

.....

.....

.....

.....

.....

.....

Devoir 2 : Établir le contexte du SMSI

Sur la base de l'étude de cas, *e-Scooter* a décidé de mettre en place d'un SMSI conformément à la norme ISO/IEC 27001 après quelques incidents de sécurité. En tant que membre de l'équipe de projet SMSI, vous êtes chargé d'identifier les exigences de conformité auxquelles *e-Scooter* doit répondre et d'identifier certains de ses biens informationnels critiques et processus opérationnels. Dressez la liste d'au moins deux éléments pour chacun d'eux.

Exigences de conformité 1 : .....

.....

.....

.....

Exigences de conformité 2 : .....

.....

.....

.....

Actif informationnel 1 : .....

.....

.....

.....

Actif informationnel 2 : .....

.....

.....

.....

Actif informationnel 3 : .....

.....

.....

.....

Processus métier 1 : .....

.....

.....

.....

Processus métier 2 : .....

.....

.....

.....

.....

Processus métier 3 : .....

.....

.....

.....

Devoir 3 : Définition du domaine d'application

Sur la base de l'étude de cas, établir le domaine d'application du SMSI d'*e-Scooter* et déterminer ses limites. La direction générale souhaite que le domaine d'application soit perçu comme ayant une valeur ajoutée pour ses clients et, parallèlement, le délimiter autant que possible pour la certification initiale du SMSI.

Périmètre :

.....

.....

.....

.....

Explication et justification :

.....

.....

.....

.....

Définir les limites organisationnelles :

.....

.....

.....

.....

Définir les limites des systèmes d'information :

.....

.....

.....

.....

Définir les limites physiques :

.....

.....

.....

.....

.....

Exercice 2 : Identification des menaces et des vulnérabilités

Déterminez les menaces et les vulnérabilités associées aux scénarios suivants. De plus, indiquer si les conséquences affecteraient la confidentialité, l'intégrité ou la disponibilité des renseignements de l'organisme.

1. Les résultats de l'audit interne ont révélé que les informations d'identification de l'utilisateur d'un ancien employé étaient toujours utilisées.
2. Un employé a fait une mauvaise valeur d'entrée dans l'interface de ligne de commande du serveur de développement qui a arrêté tout le serveur.
3. La version améliorée de l'application a été perdue lorsqu'il s'est avéré qu'un ensemble de disques durs installés dans les machines des développeurs étaient défectueux.

Complétez la matrice des risques et préparez-vous à discuter de vos réponses.

Devoir 4 : Analyse des écarts

Scénarios de risque	Menace	Vulnérabilité	Conséquences	C	I	A
Les résultats de l'audit interne ont révélé que les informations d'identification de l'utilisateur d'un ancien employé étaient toujours utilisées.						
Un employé a fait une mauvaise valeur d'entrée dans l'interface de ligne de commande du serveur de développement qui a arrêté tout le serveur.						
La version améliorée de l'application a été perdue lorsqu'il s'est avéré qu'un ensemble de disques durs installés dans les machines des développeurs étaient défectueux.						

En vous référant à l'étude de cas, évaluez le niveau de maturité du processus d'accès aux données clients stockées dans la blockchain. En outre, fournir des recommandations pour l'amélioration du processus, afin que l'entreprise réponde aux exigences de la mesure 5.15 *Contrôle d'accès* de la norme ISO/IEC 27001.

.....

.....

.....

.....

.....

Devoir 5 : Rédiger une politique de sécurité :
Suite à un incident récent de sécurité de l'information dans l'entreprise, *e-Scooter* a décidé d'établir une politique pour contrôler l'utilisation de tous les appareils de communication (p. ex., smartphones, tablettes et autres formes d'appareils de communication portables) sur le lieu de travail.

Pour rédiger la politique d'utilisation du smartphone, remplissez le modèle fourni ci-dessous.

POLITIQUE D'UTILISATION DES SMARTPHONES	
Introduction	
Objectif	
Domaine d'application	
Principes	
Responsabilités	
Principaux résultats	
Sanctions	
Politiques connexes	

Devoir 6 : Options de traitement des risques

Après avoir mené une évaluation approfondie des risques, le chef de projet a identifié une préoccupation importante en matière de sécurité de l'information au sein de l'entreprise dans laquelle il travaille. Il est révélé que 0,5 % des transactions électroniques, qui se traduisent par un chiffre d'affaires de 10 millions de dollars, effectuées au moyen de cartes de crédit sur l'application de l'entreprise sont susceptibles d'avoir un accès non autorisé et de potentielles violations de données. Cela représente une menace à la fois pour les aspects financiers de l'entreprise et pour la confidentialité et l'intégrité des données clients. La direction générale de l'entreprise doit prendre une décision importante sur la façon d'aborder et d'atténuer les problèmes identifiés.

Proposez quatre options de réponse au risque et dressez la liste des activités à mener en fonction de ces options.

Option 1 :

.....

.....

.....

Option 2 :

.....

.....

.....

Option 3 :

.....

.....

.....

Option 4 :

.....

.....

.....

Devoir 7 : Surveillance et révision du processus de gestion des risques

Sur la base de l'étude de cas, expliquez pourquoi il est important pour *e-Scooter* de surveiller et de passer en revue son processus de gestion des risques. Citez trois risques auxquels l'entreprise serait confrontée si elle ne prenait pas de telles mesures.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice 3 : Mesures de sécurité

Fournir un plan d'action comprenant au moins deux mesures à prendre pour assurer la conformité aux articles et mesures de sécurité ci-après de la norme ISO/IEC 27001.

Exemple : **Annexe A 8.8** ***Gestion des vulnérabilités techniques***

- *Mettre en place un processus systématique d'évaluation régulière de la vulnérabilité de l'infrastructure informatique, des applications et des composants réseau.*
- *Développez un processus robuste de gestion des correctifs pour appliquer rapidement des correctifs de sécurité et des mises à jour aux systèmes d'exploitation, applications et logiciels. Ce processus devrait comprendre des tests en temps opportun et le déploiement de correctifs pour minimiser les risques d'exploitation par des acteurs malveillants.*

1. Article 7.2 *a) l'organisme détermine la compétence nécessaire de la ou des personnes qui font du travail sous son contrôle et qui influe sur son rendement en matière de sécurité de l'information.*

.....

.....

.....

.....

2. Article 10.2 *a) Lorsqu'une non-conformité survient, l'organisme doit réagir à la non-conformité.*

.....

.....

.....

.....

3. Annexe A 8.6 *Dimensionnement*

.....

.....

.....

.....

4. Annexe A 8.7 *Protection contre les logiciels malveillants*

.....

.....

.....

.....

5. Annexe A 5.14 *Transfert de l'information*

.....

.....

.....

.....

Devoir 8 : Gestion des informations documentées

Afin de maintenir la sécurité de l'information à un niveau approprié pendant les perturbations, *e-Scooter a* décidé de mettre en œuvre, entre autres, l'annexe A 5.29 sécurité *de l'information pendant les perturbations* de l'ISO/IEC 27001. Fournir une liste des documents (au moins trois) qui devraient être produits pour assurer la conformité à l'annexe A 5.29.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Devoir 9 : Mise en œuvre des mesures

e-Scooter veut appliquer la flexibilité pour payer à la fois en ligne et en espèces. Quelles mesures l'entreprise doit-elle prendre pour assurer la sécurité des informations lorsque les clients souhaitent payer en ligne et saisir des informations personnelles afin d'effectuer des paiements directement via leurs comptes bancaires ?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Devoir 10 : Programme de sensibilisation et de formation

Sur la base de l'étude de cas, *e-Scooter* a fourni des sessions de formation et de sensibilisation liées à la sécurité de l'information uniquement à l'équipe de développement logiciel. Cela pourrait entraîner l'incapacité d'autres employés au sein de l'entreprise à prévenir les atteintes à la sécurité de l'information et les cyberattaques.

Expliquer l'importance d'organiser des programmes de formation et de sensibilisation dans une entreprise et proposer des mesures à prendre pour que les programmes de formation et de sensibilisation soient efficaces.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Devoir 11 : Constatations d'audit

Un audit interne a été réalisé par l'auditeur interne d'*e-Scooter* afin d'obtenir des informations sur l'efficacité de la mise en œuvre du SMSI et sur sa conformité aux exigences de l'entreprise pour son SMSI et aux exigences de la norme ISO/IEC 27001. Sur la base de l'étude de cas, identifiez trois constatations qui mettent en évidence la mise en œuvre efficace du SMSI et le respect des exigences ISO/IEC 27001.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice 4 : Élaboration d'indicateurs de rendement

Fournir deux indicateurs qui aideraient à évaluer les résultats d'un organisme en ce qui concerne la mise en œuvre des exigences et mesures de sécurité énoncées dans la norme ISO/IEC 27001.

Exemple : Article 5.1 Leadership et engagement

- *Nombre de réunions d'examen de la gestion tenues*
- *Taux moyen de participation aux réunions d'examen de la gestion*

1. Article 10.2 *Non-conformité et mesures correctives*

.....

.....

2. Annexe A 5.3. *Rôles, responsabilités et pouvoirs organisationnels*

.....

.....

3. Annexe A A 5.9 *Inventaire des informations et autres actifs associés*

.....

.....

4. Annexe A 5.17 *Information d'authentification*

.....

.....

Devoir 12 : Revue de direction

Expliquer le but d'un examen de la gestion, en expliquant les facteurs essentiels qui doivent faire l'objet d'un examen approfondi au cours de l'examen. En outre, fournissez les étapes clés nécessaires pour préparer un examen de gestion.