3. RISQUES 

Question récurrente : Est-ce que l'affirmation suivante est plutôt une menace ou une opportunité ?

RISQUE 01 Le plus important est que la stratégie de l'entreprise ait été établie dans le passé
Menace § 4.1 ★★★
Tous les trois ans en moyenne, il convient de vérifier l'adéquation de la stratégie au contexte de l'entreprise, aux attentes et besoins des parties prenantes. Menace car la date de l'élaboration de la stratégie n'est pas précisée

RISQUE 02 Le contexte de l'entreprise est un élément qui peut être pris en considération (même si le chef a oublié de le dire)
Menace § 4.1 ☆☆
C'est une exigence de la norme et c'est incontournable. Cela fait partie des premiers travaux à réaliser puisque la validation de la stratégie de l'entreprise en dépend

RISQUE 03 Chercher à anticiper l'évolution des attentes du client est du temps perdu (si c'est le chef qui le dit)
Menace § 4.2 ★
L'objectif de l'entreprise étant de satisfaire durablement ses clients, connaître les évolutions des attentes est un facteur clé de succès pour l'avenir

4. QCM (questionnaire à choix multiples)

QCM 01 Des affirmations suivantes, laquelle est correcte ?

1. Un produit peut être certifié ISO 27001
2. Un service peut être certifié ISO 27001
3. Le système de management de la sécurité de l'information d'une entreprise peut être certifié ISO 27001
4. Toute entreprise de plus de 100 personnes doit être certifiée ISO 27001

§ 0.1 ★

Un produit est certifié d'un point de vue technique d'après un référentiel tel que CE 023 pour un appareil médical par exemple. Seul, le système de management de la sécurité de l'information d'une entreprise peut être certifié ISO 27001. La certification est volontaire pour toute entreprise quel qu'en soit la taille

QCM 02 La première édition de la norme ISO 27001 est apparue en :

1. 1995
2. 1996
3. 2005

Avant-propos ★

1995 c'est la première version de la norme BS 7799. 1996 c'est la première version de la norme ISO 13335

QCM 03 La confidentialité c'est la propriété d'une information d'être : (même si le chef n'a pas d'opinion) **:**

1. Accessible aux seules personnes autorisées
2. Utilisable en temps voulu
3. Non altérée
4. Pour un usage interne

§ 3.10 ☆☆

Définition de l'ISO 27000 version 2018. 2. C'est la disponibilité. 3. C'est l'intégrité. 4. C'est une classification d'une information, cf. Annexe A.5.

QCM QCM QCM QCM QCM

PRATIQUES PRATIQUES PRATIQUES PRATIQUES PRATIQUES

5. PRATIQUES 

Question récurrente : Est-ce que l'affirmation suivante est plutôt une bonne pratique ou un écart à éviter ?

PRATIQUE 01 Le diagnostic du contexte de l'entreprise comprend les principaux enjeux externes et internes (même si le chef n'est pas au courant)

Bonne pratique § 4.1 ★

Pour comprendre le contexte de l'entreprise, la direction doit déterminer en priorité les enjeux internes et externes

PRATIQUE 02 Pour déterminer les enjeux du contexte, l'analyse de l'environnement concurrentiel est prioritaire

Écart à éviter § 4.1 ★

La direction doit d'abord déterminer les enjeux internes et externes

PRATIQUE 03 L'analyse des besoins et des attentes des parties prenantes est indépendante des produits et services de l'entreprise

Écart à éviter § 4.2 ☆☆

Les produits et les services de l'entreprise doivent prendre en compte les besoins et les attentes des parties prenantes

6. CAS 

CAS 01 CONTEXTE

Situation : les enjeux externes et internes exercent une influence sur l'orientation stratégique et la performance globale de l'entreprise

Défi : comment comprendre l'influence des enjeux externes et internes ?

Solution 1 : surveiller et passer en revue régulièrement les enjeux

Solution 2 : déterminer l'influence positive ou négative de chaque enjeu

Solution 3 : utiliser les outils SWOT et PESTEL

§ 4.1 ★★★

Toutes ces activités sont très utiles pour analyser le contexte

CAS 02 CLIENTS ET BESOINS

Situation : depuis quelques mois l'entreprise connaît une stagnation des ventes. Les non-conformités commencent à remplir la prison

Défi : quelle solution choisir pour inverser la situation ?

Solution 1 : se démarquer de la concurrence avec des prix très bas

Solution 2 : recruter un commercial sortant d'une grande école

Solution 3 : aller au contact des clients et identifier le problème

§ 4.2 ★

Trouver les causes des non-conformités, mettre en place un plan d'action, discuter franchement avec les clients, comprendre leurs besoins et attentes est une condition préalable au redressement de l'entreprise

Pratiquer des prix très bas est audacieux mais ce n'est pas une garantie de succès et peut avoir des conséquences financières désastreuses

Un nouveau commercial peut apporter des bénéfices mais cela prend beaucoup de temps et demande un investissement conséquent

CAS 03 DOMAINE D'APPLICATION DU SMSI

Situation : nous devons tenir à jour le domaine d'application du SMSI sous la forme d'une information documentée

Défi : que faire pour déterminer le domaine d'application du SMSI ?

Solution 1 : justifier chaque exigence non applicable dans une information documentée

Solution 2 : tenir à jour le domaine d'application du SMSI (les sites, les processus, les produits et services) comme information documentée

Solution 3 : prendre en compte les exigences des parties prenantes et les produits et services fournis

§ 4.3 ★

Toutes ces activités sont utiles pour déterminer le domaine d'application du SMSI