PECB

QUIZ

FORMATION CERTIFIED
ISO/IEC 27001 LEAD IMPLEMENTER

1. **Que fournit ISO/IEC 27001 ?**
   A. Lignes directrices pour la mise en œuvre d'un système de management de la sécurité de l'information
   B. Exigences pour la mise en œuvre d'un système de management de la sécurité de l'information
   C. Lignes directrices et exigences relatives à la mise en œuvre d'un système de gestion des renseignements personnels

2. **Laquelle des affirmations suivantes est correcte ?**
   A. Les organismes peuvent obtenir une certification conformément à ISO/IEC 27001
   B. Les organismes peuvent obtenir une certification conformément à ISO/IEC 27003
   C. Les organismes peuvent obtenir une certification conformément à ISO/IEC 27005

3. **Laquelle des normes suivantes fournit un ensemble de référence de mesures de sécurité de l'information et des lignes directrices pour leur mise en œuvre ?**
   A. ISO/IEC 27002
   B. ISO/IEC 27701
   C. ISO/IEC 27005

4. **Dans quels domaines ISO/IEC 27001 et le Règlement général sur la protection des données (RGPD) se chevauchent-ils ?**
   A. Collecte et traitement des IPI et droits des personnes concernées
   B. Confidentialité, disponibilité et intégrité des données, et appréciation du risque
   C. Sécurité physique, contrôle d'accès et amélioration continue

5. **Que signifie STAR, un programme d'assurance des fournisseurs de cloud à trois niveaux ?**
   A. Security, Trust, Assurance, and Risk
   B. Sécurité, tâche, action et résultats
   C. Sécurité, transparence, assurance et réponse

Quiz 2 : Système de management de la sécurité de l'information (SMSI)

1. **Un système de gestion est un ensemble d'éléments interdépendants ou interactifs d'un organisme pour établir des politiques, des objectifs et des processus pour atteindre ces objectifs.**
   A. Vrai
   B. Faux

2. **Qu'appelle-t-on système de management intégré (SMI) ?**
   A. Il s'agit d'un système de management qui intègre toutes les lignes directrices et les bonnes pratiques afin de permettre la réalisation de son objectif et de sa mission.
   B. Il s'agit également d'un système de management qui intègre toutes les composantes d'une entreprise dans un système cohérent afin de permettre la réalisation de son objectif et de sa mission.
   C. C'est aussi un système de management qui intègre tous les cadres et toutes les ressources afin de permettre la réalisation de son objectif et de sa mission.

3. **Lequel des éléments suivants est un avantage d'un SMSI efficace ?**
   A. Réduire les risques liés à la sécurité de l'information
   B. Éliminer complètement les risques liés à la sécurité de l'information
   C. Prévenir toutes les violations de données

4. **L'annexe A de la norme ISO/IEC 27001 se compose de 114 mesures de sécurité réparties en cinq thèmes.**
   A. Vrai
   B. Faux

5. **Comment l'approche processus est-elle définie ?**
   A. Une approche systématique de la sécurité de l'information d'un organisme pour atteindre ses objectifs opérationnels
   B. Intégration du SMSI dans le contexte des activités et processus commerciaux dans l'ensemble de l'organisme
   C. Identification et gestion ordonnée des processus au sein d'un organisme

Quiz 3 : Concepts et principes fondamentaux de la sécurité de l'information

1. **Lequel des éléments suivants est considéré comme un bien organisationnel virtuel ?**
   A. Comptes de messagerie
   B. Propriété intellectuelle
   C. Identité client numérique

2. **Laquelle des affirmations suivantes concernant la sécurité de l'information est exacte ?**
   A. La sécurité de l'information implique la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information, quels que soient son type et sa forme
   B. La sécurité de l'information implique la protection de la confidentialité, de l'intégrité et de la disponibilité des données numériques uniquement
   C. La sécurité de l'information implique la protection de la confidentialité, de l'intégrité et de la disponibilité des données physiques uniquement

3. **Qu'exige la confidentialité ?**
   A. Que seuls les utilisateurs autorisés ont accès à des informations protégées et sensibles
   B. Ces informations sont exactes et complètes et ne sont pas modifiées pendant le stockage ou le transit
   C. Ces informations sont accessibles quand, où et selon les besoins et à la personne qui en a besoin

4. **Laquelle des propositions suivantes n'est PAS un exemple de menace ?**
   A. Vol de supports ou de documents
   B. Données non chiffrées
   C. Utilisation non autorisée d'un système

5. **Quel principe de sécurité de l'information serait susceptible d'être affecté par une interruption de service ?**
   A. Disponibilité
   B. Confidentialité
   C. Intégrité

6. **La vulnérabilité est une faiblesse d'un bien ou d'une mesure de sécurité exploitable par une ou plusieurs menaces.**

A. Vrai
B. Faux

7. **La répartition des tâches, la rotation des postes et les processus d'approbation sont quels types de mesures ?**
   A. Mesures techniques
   B. Mesures managériales
   C. Mesures administratives

8. **Quelle est la fonction de la mesure pour la séparation des environnements de développement, de test et d'exploitation ?**
   A. Préventive
   B. Détective
   C. Corrective

9. **Un organisme a installé des systèmes d'alarme dans ses locaux. Quel type de mesure est-ce, et quelle fonction a-t-elle ?**
   A. Administrative, préventive
   B. Managériale, corrective
   C. Technique, de détection

10. **Les biens peuvent avoir _____ qui peuvent être exploités par _____.**
    A. Menaces, vulnérabilités
    B. Vulnérabilités, menaces
    C. Menaces, risques

Quiz 4 : Démarrage de la mise en œuvre du SMSI

1. **Quelle approche de mise en œuvre comprend l'application des meilleures pratiques en matière de gestion de projet ?**
   A. Approche commerciale
   B. Approche itérative
   C. Approche systématique

2. **Quelle est la définition exacte du terme projet ?**
   A. Un processus unique consistant en un ensemble d'activités coordonnées et contrôlées pour atteindre un objectif conforme à des exigences spécifiques
   B. Le plus petit objet de travail identifié dans un organisme
   C. Processus de planification, d'organisation, de contrôle et de rapport d'un ensemble d'activités visant à atteindre les objectifs

3. **Laquelle des déclarations suivantes concernant le SMSI est correcte ?**
   A. De nouvelles technologies devraient être intégrées lors de la mise en œuvre du SMSI afin d'optimiser les processus
   B. Les rôles et responsabilités des parties intéressées concernant le SMSI devraient être définis après le processus de mise en œuvre
   C. Le SMSI doit être intégré aux processus existants de l'organisme

4. **Lequel des facteurs suivants n'est PAS déterminant pour la mise en œuvre d'un SMSI ?**
   A. Niveau de maturité des mesures et des processus
   B. Lois et règlements spécifiques
   C. Dépendance à la technologie

5. **Quelle est l'approche itérative ?**
   A. Mise en œuvre globale des processus de SMSI, et non en isolant certains processus.
   B. Mise en œuvre rapide du SMSI en respectant les exigences minimales de la norme et en procédant ensuite à une amélioration continue.
   C. Harmonisation du SMSI avec d'autres systèmes de gestion établis au sein de l'organisme

Quiz 5 : Compréhension de l'organisme et de son contexte

1. **Pourquoi est-il important de comprendre la mission, les objectifs, les valeurs et les stratégies d'un organisme ?**
   A. Pour faciliter le processus d'audit interne
   B. Pour créer une carte de tous les processus
   C. Assurer un alignement cohérent avec les objectifs de sécurité de l'information

2. **Qu'exige, entre autres, l'ISO/IEC 27001 pour établir des objectifs en matière de sécurité de l'information ?**
   A. Impliquer toutes les parties prenantes
   B. Conserver les informations documentées
   C. Évaluer leur réalisation tous les trimestres

3. **_____ est une personne ou un organisme qui peut avoir une incidence sur une décision ou une activité, en être affecté ou s'en apercevoir.**
   A. Un client
   B. Une partie intéressée
   C. Un fournisseur

4. **Lequel des éléments suivants n'est PAS un élément à prendre en considération lors de l'analyse du contexte interne de l'organisme ?**
   A. Concurrents
   B. Gouvernance et structure organisationnelle
   C. Flux d'informations et processus décisionnels

5. **Quelles sont les exigences suivantes des parties intéressées que les organismes doivent prendre en considération, conformément à l'article 4.2 de la norme ISO/IEC 27001 ?**
   A. Exigences légales et réglementaires
   B. Exigences relatives aux changements climatiques
   C. À la fois A et B

Quiz 6 : Domaine d'application du SMSI

1. **Quels facteurs peuvent affecter le domaine d'application du SMSI, entre autres ?**
   A. Fonctions d'assistance, telles que services informatiques et applications logicielles
   B. Les fonctions externalisées
   C. À la fois A et B

2. **Lorsqu'il détermine le domaine d'application du SMSI, l'organisme doit tenir compte des interfaces et des dépendances entre les activités qu'il effectue et celles réalisées par d'autres organismes.**
   A. Vrai
   B. Faux

3. **Quelles sont les dimensions suivantes à prendre en considération pour définir les limites du domaine d'application du SMSI ?**
   A. Limites du système d'information
   B. Limites physiques
   C. À la fois A et B

4. **Quelles limites du SMSI l'organisme peut-il déterminer en évaluant les responsabilités des décideurs et leurs domaines d'influence ?**
   A. Organisationnelles
   B. Matérielles
   C. Système d'information

5. **Laquelle des déclarations suivantes concernant le domaine d'application du SMSI est correcte ?**
   A. Le domaine d'application du SMSI devrait être classé parmi les informations confidentielles
   B. Le domaine d'application du SMSI n'a pas à prendre en considération les besoins et les attentes des parties intéressées
   C. Le domaine d'application du SMSI doit être disponible sous forme d'informations documentées

6. **Quel est le processus recommandé pour apporter des modifications au domaine d'application du SMSI ?**
   A. Les modifications doivent être mises en œuvre automatiquement si l'organisme est certifié par un organisme d'évaluation de la conformité (CAB)
   B. Les changements doivent être justifiés et approuvés lors d'un examen de gestion
   C. Les changements doivent être documentés et approuvés uniquement par le gestionnaire de projet du SMSI

Quiz 1 basé sur un scénario

YoMedia est une société d'insights basée à Milan, en Italie, qui fournit des services de recherche dans le monde entier. L'entreprise collecte, analyse et interprète les données clients pour offrir des solutions à ses clients en fonction des résultats. En raison de la nature de leurs services, les dirigeants de *YoMedia ont* décidé de mettre en place un système de management de la sécurité de l'information (SMSI) basé sur les exigences de la norme ISO/IEC 27001 afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information. En outre, en tant qu'entreprise opérant au sein de l'Union européenne (UE), *YoMedia* s'engage à respecter le Règlement général sur la protection des données (RGPD) afin de protéger les droits à la vie privée de ses clients.

Pour mettre en œuvre efficacement le SMSI et assurer la conformité au RGPD, *YoMedia* a mobilisé une équipe SMSI dédiée. L'équipe comprenait des membres de divers départements, notamment les départements informatique, juridique, conformité et assistance à la clientèle. Leur responsabilité était de mettre en œuvre efficacement le SMSI et d'assurer la conformité au RGPD.

Dans un premier temps, l'équipe du SMSI a identifié tous les systèmes et processus qui traitent les données et informations des clients, assurant ainsi leur inclusion dans le domaine d'application du SMSI. Le domaine d'application couvrait les aspects organisationnels, informatiques et de communication, ainsi que les aspects physiques. Pour définir les limites du SMSI, l'équipe a utilisé l'approche consistant à adopter les limites utilisées par les utilisateurs eux-mêmes. Ils ont également pris en compte les frontières géographiques et temporelles.

De plus, l'équipe du SMSI a procédé à une analyse approfondie des forces et des faiblesses de *YoMedia* dans le but de déterminer où l'organisme devrait investir ses ressources. L'équipe a mené des entrevues avec les employés de l'entreprise et a utilisé diverses techniques pour recueillir de l'information sur les processus, procédures, politiques et mesures de sécurité existants. Au cours de l'analyse, l'équipe a découvert que *YoMedia* utilise un logiciel de contrôle d'accès qui permet uniquement aux utilisateurs autorisés d'accéder aux informations sensibles. Cependant, leur application logicielle et leurs programmes ont une interface utilisateur compliquée qui se traduit par un grand nombre d'erreurs d'entrée de données par le personnel au quotidien. De plus, en menant des entrevues, ils ont appris qu'il y avait plusieurs employés de différents ministères qui n'avaient reçu aucune formation en sécurité.

Sur la base de leurs conclusions, l'équipe du SMSI a conclu que l'entreprise doit redéfinir ses besoins en formation et simplifier son interface utilisateur pour répondre efficacement aux problèmes identifiés.

Répondez aux questions suivantes en vous référant au scénario ci-dessus :

1. **En utilisant les limites privilégiées par les utilisateurs, quelle approche l'équipe du SMSI a-t-elle utilisée pour définir les limites organisationnelles ?**
   A. L'approche réaliste
   B. L'approche commune
   C. L'approche ad hoc

2. **L'équipe du SMSI a utilisé la méthode des limites temporelles. Que comprend cette méthode ?**
   A. Programmes de temps et de bureau
   B. Bureaux de l'organisme
   C. À la fois A et B

3. **Laquelle des situations présentées dans le scénario est considérée comme une menace pour la sécurité de l'information ?**
   A. Erreur d'entrée des données par le personnel
   B. Interface utilisateur compliquée
   C. Utilisation quotidienne de programmes ou d'applications par le personnel.

4. **Quelle approche l'équipe du SMSI a-t-elle appliquée pour analyser le contexte de l'organisme ?**
   A. Analyse PEST
   B. Analyse des cinq forces de Porter
   C. Analyse SWOT

5. **Plusieurs employés de différents départements de *YoMedia* n'ont reçu aucune formation en sécurité. Qu'est-ce que cela indique ?**
   A. La présence d'une menace liée aux fonctions possibles de l'entreprise.
   B. La présence d'un risque pour la sécurité de l'information exprimée comme la combinaison de l'impact et de la survenue d'un incident dans l'entreprise
   C. La présence d'une vulnérabilité dans les procédures existantes de l'entreprise en matière de personnel

Quiz 7 : Leadership et approbation du projet

1. **Quelles ressources sont habituellement nécessaires à la mise en œuvre d'un SMSI, entre autres ?**
   A. Marketing, ventes, publicité
   B. Systèmes de gestion d'inventaire et équipement de fabrication
   C. Personnes, informations, installations, finances

2. **Pourquoi certains projets dans des environnements hautement concurrentiels accordent-ils la priorité à une planification initiale minimale ?**
   A. Tenir compte des commentaires des intervenants et des nouvelles technologies
   B. Pour minimiser le coût du retard et accélérer la mise sur le marché
   C. Évaluer les effets environnementaux et éclairer les décisions de conception en matière de durabilité

3. **Que doit inclure un plan de projet SMSI ?**
   A. Problèmes courants et décisions en attente
   B. Tous les projets et sous-projets actuels avec leurs jalons
   C. À la fois A et B

4. **Une équipe de projet SMSI est généralement composée du porteur du projet, du gestionnaire de projet, de l'équipe de gestion de projet, de l'équipe de projet et des parties intéressées.**
   A. Vrai
   B. Faux

5. **Qui devrait approuver la mise en œuvre du SMSI ?**
   A. Toutes les parties intéressées
   B. La direction générale de l'organisme
   C. Le responsable du département informatique

Quiz 8 : Structure organisationnelle

1. **Selon la norme ISO/IEC 27001, qui doit s'assurer que les responsabilités et les pouvoirs pour les rôles liés à la sécurité de l'information sont attribués et communiqués ?**
   A. Ressources humaines
   B. Direction générale
   C. Chefs de départements

2. **Quel est le principal avantage de la structure organisationnelle traditionnelle ?**
   A. Séparation claire entre les rôles et responsabilités de la sécurité de l'information et de l'informatique
   B. Les questions ne concernent que la sécurité stratégique et les aspects non technologiques
   C. La technologie et la sécurité de l'information font partie d'un même département

3. **Quel est le rôle du comité exécutif dans le cadre du SMSI ?**
   A. Organisation de réunions quotidiennes avec des employés pour discuter de questions liées à la sécurité de l'information
   B. Rôle d'orientation, de contrôle, de validation, de prise de décision et d'arbitrage pour le SMSI
   C. Établir des fréquences minimales de réunion pour tous les comités au sein de l'organisme

4. **Lequel des éléments suivants n'est PAS un comité clé du projet de mise en œuvre du SMSI d'un organisme ?**
   A. Comité de sécurité de l'information
   B. Comité opérationnel
   C. Comité des parties prenantes

5. **Qui est le principal responsable du bon fonctionnement du SMSI et des mesures de sécurité ?**
   A. L'auditeur interne
   B. Le comité de sécurité de l'information
   C. Le comité opérationnel

Quiz 9 : Analyse du système existant

1. **Qu'est-ce qu'une analyse des écarts ?**
   A. Une technique utilisée pour déterminer les étapes à suivre pour passer d'un état actuel à un état futur souhaité.
   B. Une technique utilisée pour déterminer les façons dont un processus peut potentiellement échouer, dans le but d'éliminer la probabilité d'un tel échec.
   C. Une technique utilisée pour évaluer l'organisme par rapport à ses concurrents afin d'établir une stratégie globale à long terme

2. **Un organisme a signalé que ses processus ont atteint un niveau de qualité supérieure à la suite d'une amélioration continue et de la conformité aux pratiques exemplaires. De quel niveau de maturité s'agit-il ?**
   A. Gérés quantitativement
   B. Optimisés
   C. À l'état initial

3. **Lequel des éléments suivants N'est PAS un niveau de maturité ?**
   A. Gérés
   B. Optimisés
   C. Définis

4. **Laquelle des méthodes suivantes N'est PAS utilisée pour recueillir des renseignements sur le système de gestion actuel d'un organisme ?**
   A. Examen des États financiers et des dossiers fiscaux de l'organisme
   B. Envoyer un questionnaire à un échantillon de personnes qui sont représentatives des parties intéressées
   C. Utilisation d'outils d'analyse pour détecter les vulnérabilités techniques et établir une liste des biens du réseau

5. **Lequel des éléments suivants est un outil visuel efficace que les organismes peuvent utiliser pour présenter les résultats de l'analyse des écarts ?**
   A. Carte radar
   B. Diagramme d'Ishikawa
   C. Diagrammes de causes et effets

Quiz 10 : Politique de sécurité de l'information

1. **Selon ISO/IEC 27001, qui est responsable de l'élaboration de la politique de sécurité de l'information ?**
   A. La direction générale
   B. Le chef de projet SMSI
   C. Le responsable de la sécurité de l'information

2. **Quelle est la différence entre une politique et une directive ?**
   A. Une politique énonce les intentions et l'orientation d'un organisme, tandis qu'une directive indique comment quelque chose doit être fait.
   B. Une politique est un type de directive qui fournit des recommandations sur différents sujets.
   C. Il s'agit également d'un document qui indique comment quelque chose doit être fait, alors qu'une directive est une explication des procédures.

3. **Quel type de politiques spécifie les exigences internes d'une autre politique et couvre un public cible particulier ?**
   A. Politiques générales de haut niveau
   B. Politiques spécifiques de haut niveau
   C. Politiques spécifiques à un sujet

4. **Lequel des éléments suivants est une politique spécifique de haut niveau ?**
   A. Politique de gestion des incidents
   B. Politique de sécurité de l'information
   C. Politique de cryptographie

5. **Quelle est la première phase du cycle de vie de l'élaboration d'une politique de sécurité de l'information ?**
   A. Élaboration de la politique
   B. Surveillance et maintenance de la politique
   C. Appréciation du risque

Quiz 11 : Gestion du risque (Partie 1)

1. **Que fournit ISO/IEC 27005 ?**
   A. Exigences pour la gestion des risques de la sécurité de l'information
   B. Lignes directrices pour la gestion de tout type de risque, quelle que soit sa nature ou ses conséquences
   C. Directives sur la gestion des risques en sécurité de l'information

2. **Que faut-il prendre en considération lors de la sélection d'une méthodologie d'évaluation du risque lors de la mise en œuvre d'un SMSI, entre autres ?**
   A. L'évolutivité de la méthodologie pour intégrer différentes tailles et complexités de projet
   B. Compatibilité de la méthodologie avec l'ensemble des critères de l'ISO/IEC 27001
   C. Risques résiduels documentés dans le plan de traitement des risques

3. **Lequel des éléments suivants définit le mieux les biens primaires/commerciaux dans le contexte de la sécurité de l'information d'un organisme ?**
   A. Les biens primaires/commerciaux comprennent les infrastructures physiques telles que les bâtiments et les entrepôts
   B. Les biens primaires/commerciaux sont des composantes du système d'information qui prennent en charge d'autres biens
   C. Biens primaires/commerciaux se réfèrent à l'information ou aux processus de valeur pour un organisme

4. **Quelle phase de l'appréciation du risque vise à trouver, reconnaître et décrire les risques ?**
   A. Identification des risques
   B. Évaluation du risque
   C. Analyse du risque

5. **Lequel des processus suivants consiste à comparer les résultats de l'analyse du risque avec les critères de risque pour déterminer si le risque et son ampleur sont acceptables ou tolérables ?**
   A. Traitement des risques
   B. Évaluation du risque
   C. Acceptation des risques

Quiz 12 : Gestion du risque (Partie 2)

1. **Quel processus modifie le risque ?**
   A. Évaluation du risque
   B. Identification des risques
   C. Traitement des risques

2. **L'entreprise a décidé de confier le processus de paiement à un organisme externe afin de réduire le risque. Quelle option de traitement des risques l'organisme a-t-il retenue ?**
   A. Prise de risque
   B. Partage du risque
   C. Modification des risques

3. **Le risque résiduel est le niveau de risque avant toute mesure.**
   A. Vrai
   B. Faux

4. **Qu'est-ce qu'un objectif de communication des risques ?**
   A. Promouvoir la sensibilisation et la compréhension des risques
   B. Déléguer les responsabilités en matière de gestion des risques à des tiers
   C. Hiérarchiser la gestion des risques par rapport aux objectifs organisationnels

5. **Quels sont les facteurs suivants qui peuvent influer sur les risques que les organismes doivent surveiller en permanence, entre autres ?**
   A. Nouvelles sources de risques
   B. Les changements sont des lois et des règlements
   C. À la fois A et B

Quiz 13 : Déclaration d'applicabilité

1. **Selon ISO/IEC 27001, que doit contenir la déclaration d'applicabilité ?**
   A. Les délais d'audit des mesures
   B. La justification de l'exclusion de toute mesure de l'annexe A
   C. Le nom des personnes responsables de l'efficacité des mesures

2. **Comment un organisme choisit-il les mesures de sécurité de l'ISO/IEC 27001, Annexe A ?**
   A. Sur la base des résultats de l'appréciation du risque
   B. Sur la base de la décision de la direction générale
   C. Sur la base du rapport d'audit interne

3. **La norme ISO/IEC 27001 exige que l'organisme choisisse ses mesures uniquement à partir de l'annexe A.**
   A. Vrai
   B. Faux

4. **Laquelle des raisons suivantes est commune pour exclure les mesures de l'annexe A de la norme ISO/IEC 27001 ?**
   A. Rationaliser les processus opérationnels et la réduction de la complexité de l'organisme
   B. Violation des exigences légales, légales ou contractuelles
   C. Conflits potentiels avec les meilleures pratiques et lignes directrices de l'industrie

Quiz 2 basé sur un scénario

DetSearch est une société de recherche et développement de premier plan dont le siège social est situé à Barcelone, Espagne. Elle est spécialisée dans la fourniture de solutions de données complètes qui permettent aux clients de saisir des opportunités lucratives sur le marché. Ses services comprennent des études de marché approfondies, des études de comportement des consommateurs, la prévision des tendances, l'intelligence concurrentielle, la visualisation et le reporting des données et la consultation stratégique, le tout guidé par des analyses avancées des données et des informations pour permettre aux clients de prendre des décisions éclairées et d'atteindre le succès commercial.

La direction générale de *DetSearch* a récemment décidé de donner la priorité à la conformité aux exigences légales et réglementaires en matière de sécurité de l'information. À ce titre, afin d'assurer la sécurité de l'information et de maintenir la confiance des clients estimés, la direction générale a décidé de mettre en place un système robuste de management de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001.

Alors que l'entreprise amorçait la mise en œuvre du SMSI, l'accent restait mis sur la protection des données de tous formats et sur la garantie de la confidentialité, de l'intégrité et de la disponibilité des renseignements sensibles des clients. La direction générale a confié le rôle de chef de projet SMSI à Carla, la responsable de la sécurité des systèmes d'information, en raison de son expertise en sécurité de l'information et en gestion de projet. Elle était chargée de diriger la mise en œuvre à toutes les étapes, y compris la rédaction du plan de projet du SMSI, et d'assurer l'approbation de la direction générale. En outre, la direction générale a mobilisé l'équipe SMSI composée uniquement d'experts en sécurité de l'information.

Premièrement, la direction générale a identifié les ressources nécessaires à la mise en œuvre du SMSI, y compris les systèmes d'information, de transport, de personnes, de technologies de l'information et de la communication (TIC), les installations, l'équipement et les finances. Toutefois, ils n'incluaient pas les partenaires et les fournisseurs comme ressource nécessaire, car ils ne la jugeaient pas nécessaire.

Par la suite, l'équipe du SMSI a effectué une analyse des écarts. Ils ont suivi une approche systématique, en commençant par déterminer l'état actuel de l'organisme en identifiant les processus existants et les mesures de sécurité de l'information en place. Par la suite, ils fixent des objectifs spécifiques pour chaque mesure de sécurité de l'information. Après avoir obtenu les résultats de l'analyse des écarts, Carla et l'équipe SMSI étaient bien équipées pour planifier et hiérarchiser les actions nécessaires pour

renforcer les mesures de sécurité de l'information et garantir la confidentialité, l'intégrité et la disponibilité des données dans toutes les opérations de *DetSearch*.

Ensuite, Carla a rédigé la politique de sécurité de l'information. Elle a défini les composantes de la politique, rédigé les sections de la politique et validé le contenu et le format de la politique.

L'équipe du SMSI a procédé à une évaluation du risque. Dans le cadre de l'analyse du risque, l'équipe du SMSI assure clarté et cohérence en consignant des explications claires sur les termes employés et la base de chaque critère. Ils reconnaissent l'importance d'éviter les biais individuels et les opinions divergentes, d'assurer la répétabilité et la reproductibilité en documentant les notes explicatives pour les valeurs évaluées.

Répondez aux questions suivantes en vous référant au scénario ci-dessus :

1. ***DetSearch* a créé l'équipe du projet SMSI composée uniquement d'experts en sécurité de l'information. Est-ce une bonne pratique à suivre ?**
   A. Non, si la constitution de l'équipe de projet SMSI composée uniquement d'experts en sécurité de l'information pourrait apporter des connaissances précieuses en sécurité de l'information et en technologie à *DetSearch*, ce n'est pas une bonne pratique dans son intégralité
   B. Oui, inclure des personnes d'horizons différents dans l'équipe du projet SMSI ne ferait que ralentir le processus décisionnel pour *DetSearch,* ce qui conduirait à une mise en œuvre moins efficace des mesures de sécurité
   C. Oui, le fait d'avoir une équipe composée uniquement d'experts en sécurité de l'information garantirait la bonne mise en œuvre du SMSI.

2. **Clara a identifié les ressources pour la mise en œuvre du SMSI. Est-ce une bonne pratique ?**
   A. Oui, le gestionnaire de projet du SMSI est chargé d'identifier les ressources nécessaires à la mise en œuvre du SMSI.
   B. Non, toutes les personnes concernées par le SMSI devraient participer à l'identification des ressources nécessaires à la mise en œuvre du SMSI.
   C. Non, l'équipe du SMSI devrait identifier les ressources nécessaires à la mise en œuvre du SMSI.

3. **L'équipe du SMSI a-t-elle correctement suivi l'approche systématique consistant à effectuer l'analyse des écarts ?**

A. Non, l'équipe du SMSI aurait dû d'abord se concentrer sur la fixation d'objectifs spécifiques pour chaque mesure de sécurité de l'information avant de procéder à l'analyse des écarts afin d'assurer une évaluation plus précise
B. Non, l'équipe SMSI aurait dû ignorer l'analyse des écarts, car il s'agit d'une étape inutile qui ajoute seulement de la complexité à la mise en œuvre du SMSI
C. Oui, l'équipe du SMSI a suivi correctement l'approche systématique consistant à effectuer l'analyse des écarts

4. Au cours de l'élaboration de la politique de sécurité de l'information, Carla a-t-elle suivi toutes les étapes essentielles ?

A. Non, Carla n'a pas validé la politique avec les intéressés
B. Non, Carla n'a pas envisagé l'intégration du cahier des charges opérationnel et des références à des produits spécifiques dans la politique
C. Oui, Carla a suivi toutes les étapes essentielles pour rédiger la politique

5. Quelle technique d'analyse du risque l'équipe du SMSI a-t-elle utilisée ?

A. Analyse qualitative des risques
B. Analyse semi-qualitative des risques
C. Analyse quantitative des risques

Quiz 14 : Sélection et conception des mesures

1. **Que représente l'architecture de sécurité d'un organisme ?**
   A. Ensemble de pratiques utilisées pour répondre aux exigences de sécurité au niveau tactique
   B. Ensemble de pratiques utilisées pour répondre aux exigences de sécurité au niveau opérationnel
   C. Ensemble de pratiques utilisées pour répondre aux exigences de sécurité au niveau du système

2. **Lequel des services de sécurité suivants vise à faciliter l'identification des utilisateurs et à prendre en charge l'authentification partagée dans l'ensemble de l'organisme ?**
   A. Contrôle des frontières
   B. Contrôle d'accès
   C. Cryptographie

3. **Quels sont les six niveaux en cascade couverts par la matrice SABSA pour le développement de l'architecture de sécurité ?**
   A. Éléments, but, procédures, personnel, zone et calendrier
   B. Fonctions, planification, procédures, personnel, géographie et durée
   C. Biens, motivation, processus, personnes, lieu et heure

4. **Parmi les mesures suivantes, lesquelles doivent être prises par les organismes pour préparer la mise en œuvre des mesures de sécurité de l'information, entre autres ?**
   A. Préparer les informations documentées requises
   B. Effectuer une analyse des coûts
   C. À la fois A et B

5. **Pourquoi les organismes devraient-ils associer les employés au processus d'élaboration des procédures et des politiques en matière de sécurité de l'information ?**
   A. Parce qu'il permet d'économiser du temps et des ressources pendant le processus de rédaction
   B. Parce que cela les motive à contribuer à la mise en œuvre des mesures de sécurité de l'information
   C. Parce que c'est une exigence de la norme ISO/IEC 27001

6. **La norme ISO/IEC 27001 fournit une méthode de documentation spécifique à utiliser pour la conception et la description des mesures.**
   A. Vrai
   B. Faux

Quiz 15 : Mise en œuvre des mesures

1. **Dans combien de thèmes sont regroupés les 93 mesures de l'annexe A ?**
   A. Cinq
   B. Trois
   C. Quatre

2. **Quel est le principal objectif de la mesure 6.1 *Examen préalable* de l'annexe a de la norme ISO/IEC 27001 ?**
   A. S'assurer que tous les membres du personnel sont éligibles et aptes à remplir leurs fonctions.
   B. S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités
   C. Protéger les intérêts de l'organisme dans le cadre de tout changement d'emploi.

3. **Qui devrait avoir accès à des procédures d'exploitation documentées pour les installations de traitement de l'information ?**
   A. Uniquement la direction générale
   B. Seul le responsable des procédures d'exploitation
   C. Tout utilisateur qui en a besoin

4. **Quelle est la principale exigence de la mesure 8.34 *Protection des systèmes d'information pendant les tests d'audit* de l'annexe A ?**
   A. Le testeur et la direction appropriée doivent gérer adéquatement les informations relatives aux tests
   B. Le testeur et la direction appropriée doivent planifier et convenir des tests d'audit et d'autres activités d'assurance impliquant l'évaluation des systèmes opérationnels
   C. Le testeur doit séparer et sécuriser les environnements de développement, de test et de production

5. **Quelle est la mesure 5.7 *Renseignements sur les menaces* figurant à l'Annexe A ?**
   A. Faire connaître l'environnement de menaces de l'organisme afin de prendre les mesures d'atténuation appropriées
   B. Assurer un flux approprié d'informations
   C. Veiller à ce que les risques liés à la sécurité de l'information liés aux produits livrables soient efficacement pris en compte dans la gestion de projet tout au long du cycle de vie du projet.

Quiz 16 : Gestion des informations documentées

1. **Entre autres choses, que doivent faire les organismes pour se conformer à l'article 7.5.1 *Informations documentées* de la norme ISO/IEC 27001 ?**
   A. Élaborer une procédure pour le contrôle des informations documentées
   B. Élaborer un guide pour le contrôle des informations documentées accessibles uniquement par la direction générale
   C. Développer une base de données complète pour le contrôle des informations documentées, en stockant tous les enregistrements dans un format crypté

2. **Afin de se conformer à la norme ISO/IEC 27001, les organismes devraient mettre en place un système complexe de contrôle des documents.**
   A. Vrai
   B. Faux

3. **Que décrit une procédure ?**
   A. Un aperçu des instructions spécifiques sur les mesures à prendre
   B. Une instruction détaillée sur l'utilisation ou l'installation, la maintenance ou l'exploitation de quelque chose à une description réelle des politiques
   C. Une explication détaillée du fonctionnement d'un processus

4. **Quel est le principal objectif de l'étape d'approbation dans le processus de contrôle et de gestion des documents pour le SMSI ?**
   A. Distribuer le document à toutes les parties intéressées
   B. Pour finaliser et signer les documents
   C. Identifier les opportunités d'amélioration

5. **Quels sont les avantages d'un système documenté de gestion de l'information ?**
   A. Faciliter l'accès, le référencement, la diffusion et l'archivage des documents
   B. Assurer la traçabilité des informations documentées
   C. À la fois A et B

Quiz 17 : Tendances et technologies

1. **Laquelle des options ci-dessous ne fait PAS partie des trois V du big data ?**
   A. Volume
   B. Vélocité
   C. Variance

2. **Les données structurées sont basées sur des données binaires et ne disposent pas d'un modèle de données prédéfini.**
   A. Vrai
   B. Faux

3. **Lequel des éléments suivants est un exemple de données non structurées ?**
   A. MongoDB
   B. Bases de données SQL
   C. Fichiers Microsoft Excel

4. **Lequel des éléments suivants est un avantage de l'intelligence artificielle faible ?**
   A. Tâches automatisées
   B. Résolution de problèmes
   C. Utilisation de la pensée critique

5. **Régression linéaire, arbre de décision et régression logistique sont quelques-uns des algorithmes essentiels utilisés par :**
   A. Apprentissage automatique
   B. Intelligence artificielle
   C. Cloud computing

6. **Dans lequel des modèles de déploiement cloud suivants, les mêmes ressources informatiques sont-elles partagées entre plusieurs clients ?**
   A. Cloud privé
   B. Cloud public
   C. Cloud hybride

7. **Quels services sont fournis par le fournisseur de cloud, entre autres, lors de l'utilisation de l'infrastructure en tant que service (IaaS) ?**
   A. Virtualisation et réseau
   B. Exécution et application
   C. Middleware et données

8. **Parmi les principaux impacts des nouvelles technologies en matière de sécurité de l'information figure le fait que les mots de passe ne seront plus utilisés, car la nouvelle technologie nécessite l'utilisation de méthodes d'authentification plus sécurisées, telles que l'utilisation de la biométrie, l'identité en tant que service (IDA) et l'identification rapide en ligne (FIDO)**
   A. Vrai
   B. Faux

9. **Laquelle des affirmations suivantes concernant l'apprentissage automatique est correcte ?**
   A. L'apprentissage automatique est synonyme d'intelligence artificielle et les termes peuvent être utilisés de manière interchangeable.
   B. L'apprentissage automatique fournit des services hébergés sur Internet
   C. Il existe trois types d'apprentissages automatiques : l'apprentissage automatique supervisé, l'apprentissage automatique non supervisé et l'apprentissage par renforcement

Quiz 18 : Communication

1. **Quel principe de sécurité de l'information peut compromettre la transparence lors d'une communication si elle n'est pas correctement abordée ?**
   A. Intégrité
   B. Confidentialité
   C. Disponibilité

2. **Lequel des éléments suivants est un exemple d'objectifs de communication ?**
   A. Établir une communication transparente avec les parties intéressées pour améliorer la crédibilité et la réputation
   B. Communiquer les performances du SMSI
   C. À la fois A et B

3. **Les approches ou les outils à utiliser pour mener des activités de communication dépendent en grande partie du fait que les organismes visent à consulter, comprendre, informer ou impliquer des groupes cibles.**
   A. Vrai
   B. Faux

4. **Que doivent considérer les organismes en ce qui concerne les communications pertinentes pour le SMSI ?**
   A. Type de chiffrement utilisé pour la communication, fréquence de communication et canaux de communication
   B. Localisation physique des serveurs de communication, protocoles de sécurité en place et capacité de bande passante pour les communications
   C. Le contenu de la communication, le moment de la communication, les destinataires prévus de la communication, les personnes responsables de la communication et les processus utilisés pour la communication

5. **Quel principe de communication réussie exige de fournir des informations pertinentes aux parties intéressées en utilisant des styles, un langage et des médias qui correspondent à leurs préférences et besoins, leur permettant ainsi de participer pleinement ?**
   A. Transparence
   B. Adéquation
   C. Crédibilité

Quiz 19 : Compétence et sensibilisation

1. **Comment les organismes peuvent-ils assurer la compétence des employés pour le bon fonctionnement du SMSI ?**
   A. Sur la base d'une éducation, d'une formation ou d'une expérience appropriées
   B. Sur la base d'une compréhension approfondie de la politique de sécurité de l'information
   C. Sur la base de la titularisation et de l'ancienneté au sein de l'organisme

2. **_____ est l'encouragement des employés à acquérir des _____ nouveaux ou avancés en créant des occasions d'apprentissage et de formation avec des circonstances pour déployer les résultats qui ont été acquis.**
   A. Mentorat, compétences en leadership
   B. Reconnaissance, connaissance technologique
   C. Développement, compétence

3. **Comment déterminer l'écart de compétences ?**
   A. En comparant les niveaux de compétence précédents et actuels
   B. En comparant les niveaux de compétence actuels et requis
   C. En se basant sur les résultats des programmes de sensibilisation et de formation

4. **Un employé a reçu un e-mail avec un lien qui, lorsqu'il clique dessus, le redirige vers un site Web malveillant. Le responsable informatique identifie le problème et bloque immédiatement le système de transfert des e-mails. Quelle mesure l'organisme doit-il prendre pour éviter que des situations similaires ne se reproduisent ?**
   A. Réaliser un programme de sensibilisation pour pallier l'ingénierie sociale et les risques associés aux e-mails.
   B. Réaliser un programme de formation pour informer les salariés des risques associés aux hameçonnages et spams.
   C. Réaliser un programme de sensibilisation pour pallier les problèmes liés au contrôle d'accès.

5. **Lequel des sujets suivants est un domaine principal qui devrait être abordé au cours d'un programme de sensibilisation ?**

A. La mise en œuvre d’un logiciel antivirus
B. Les informations documentées requises par le SMSI
C. L’utilisation de mots de passe

Quiz 20 : Gestion des opérations de sécurité (partie 1)

1. **Que comprend la mesure des résultats du changement ?**
   A. Générer des métriques de changement
   B. Vérifier le succès du changement
   C. Allouer le temps nécessaire à la modification

2. **Laquelle des affirmations suivantes est correcte ?**
   A. Les organisations ne peuvent pas être certifiées selon la norme ISO/IEC 27032
   B. Les organisations peuvent être certifiées selon la norme ISO/IEC 27035-1
   C. Les organisations peuvent être certifiées selon la norme ISO/IEC 27035-2

3. **Quelle norme fournit des lignes directrices sur les pratiques de sécurité aux parties prenantes du cyberespace ?**
   A. ISO/IEC 27032
   B. ISO/IEC 27035-1
   C. ISO/IEC 27035-2

4. **Qu'entend-on par équipe du centre des opérations de sécurité (SOC) ?**
   A. Un groupe de coordonnateurs de programmes de sécurité de l'information
   B. Un groupe d'experts, d'analystes de sécurité, d'ingénieurs et de responsables qui supervisent les opérations de sécurité.
   C. Groupe d'auditeurs internes qui gèrent les activités opérationnelles de l'organisme

5. **La direction générale doit s'assurer que tous les membres du domaine d'application du SMSI comprennent la valeur et l'importance d'une politique efficace de gestion des incidents de sécurité de l'information.**
   A. Vrai
   B. Faux

Quiz 21 : Gestion des opérations de sécurité (partie 2)

1. **Lors de la réception d'un rapport d'événement, le groupe de support aux opérations complète le ticket d'événement de sécurité d'informations, l'analyse et détermine sa priorité. Quel processus de gestion des incidents s'agit-il ?**
   A. Évaluation initiale et décision
   B. Détection et rapport
   C. Deuxième évaluation et confirmation d'un incident

2. **Lequel des éléments suivants relève de l'équipe de gestion des incidents ?**
   A. Élaboration et approbation de la politique de sécurité de l'information et suivi du processus d'évaluation du risque
   B. Surveillance constante des cibles, suivi et réponses proactifs et gestion des journaux
   C. Audits réguliers de la conformité de l'organisme à la norme ISO/IEC 27001 en matière d'intervention en cas d'incident

3. **Quelles sont les quatre grandes étapes de l'analyse médico-légale ?**
   A. Analyser, préparer, réviser et améliorer
   B. Comprendre, collecter, archiver et générer des rapports
   C. Collecter, examiner, analyser et signaler

4. **Que doivent faire les organismes en ce qui concerne le processus de gestion des incidents ?**
   A. Mesurez-le à l'aide d'indicateurs de performance
   B. Réévaluez-le pour identifier les mesures correctives et préventives
   C. À la fois A et B

5. **Laquelle des déclarations suivantes concernant la continuité d'activité (CA) est correcte ?**
   A. Il définit les dangers qui menacent un organisme
   B. Il traite de l'impact direct d'un événement
   C. Il s'agit d'arrêter les effets de l'incident le plus rapidement possible et de s'attaquer immédiatement à ses conséquences

Quiz 3 basé sur un scénario

Ecovista Energy Global (EVEG) est une société innovante axée sur le développement durable fondée en 2015, à Amsterdam, aux Pays-Bas. Il opère à l'international et a établi une présence significative en Europe, en Asie du Sud-est et en Amérique du Nord a*. EVEG* se spécialise dans la fourniture de solutions écologiques et écoénergétiques aux entreprises et aux industries qui cherchent à réduire leur impact négatif sur l'environnement. L'entreprise propose un large éventail de solutions d'énergies renouvelables, y compris des systèmes d'énergie solaire, des installations éoliennes et des technologies de conversion de la biomasse. Au fur et à mesure que *EVEG* a développé et étendu ses opérations à l'échelle mondiale, la sécurité de ses informations et de ses systèmes est devenue cruciale. À ce titre, la direction générale d'*EVEG* a décidé de mettre en place un système de gestion de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001. Après une évaluation complète des risques, l'équipe SMSI a identifié les mesures de sécurité de l'information de l'annexe A de la norme ISO/IEC 27001 qui étaient essentielles à la posture de sécurité de l'organisme.

Pour protéger ses données sensibles, l'équipe SMSI a mis en place des systèmes robustes de contrôle d'accès pour s'assurer que les employés n'ont accès qu'aux informations nécessaires à leurs rôles. En outre, l'authentification multifacteurs (AMF) a également été introduite pour les comptes privilégiés, afin de réduire davantage le risque d'accès non autorisé. De plus, *il* a reconnu l'importance de séparer les tâches et responsabilités conflictuelles au sein de l'organisme. Dans le cadre des mesures de sécurité, la direction générale s'est assurée que les rôles et responsabilités des employés sont clairement définis, et que les tâches conflictuelles sont séparées pour prévenir les abus potentiels ou l'accès non autorisé à des renseignements sensibles.

L'équipe du SMSI s'est également penchée sur la nécessité de maintenir la sécurité de l'information à un niveau approprié pendant les perturbations. L'équipe SMSI a déterminé que les imprévus, tels que les catastrophes naturelles, les cyberattaques ou les défaillances du système, peuvent potentiellement avoir un impact sur les opérations et LA sécurité de l'information d'*EVEG*. C'est pourquoi *l'équipe du SMSI* a soigneusement planifié et préparé ces perturbations, veillant à ce que la sécurité de l'information reste robuste et efficace, même dans des circonstances difficiles.

L'équipe SMSI détermine également qu'il est essentiel de conserver des copies de sauvegarde des informations, des logiciels et des systèmes. À ce titre, il a établi une politique complète et spécifique au sujet de la sauvegarde, en veillant à ce que les copies de sauvegarde régulières soient créées et maintenues en toute sécurité.

Outre l'accent mis sur les contrôles d'accès, l'authentification multi-facteurs et la planification des situations d'urgence, *l'équipe SMSI* a donné la priorité à la protection de la précieuse propriété intellectuelle d'*EVEG* et à l'utilisation sécurisée des informations sensibles. L'équipe a décidé de mettre en place des mesures de sécurité qui définissent des règles efficaces pour l'utilisation des techniques cryptographiques, notamment la gestion des clés cryptographiques. En outre, *pour* protéger les droits de propriété intellectuelle, l'équipe a mis en place des procédures appropriées pour protéger ses biens intellectuels précieux contre l'utilisation non autorisée, la reproduction ou la violation.

L'équipe du SMSI n'a pas procédé à une analyse approfondie des coûts pour la mise en œuvre des mesures de sécurité. Ainsi, elle a alloué des ressources insuffisantes dans certains domaines. L'équipe a rencontré des difficultés pour définir et mettre en œuvre efficacement les règles de gestion des clés cryptographiques, compromettant la sécurité de ses informations sensibles. Le manque de ressources et de préparation a également entraîné des écarts dans ses procédures de sauvegarde et de recouvrement. En conséquence, l'entreprise n'a pas été en mesure de tester l'efficacité des procédures de sauvegarde qui garantiraient la récupérabilité des données et des systèmes en cas de perturbations.

Répondez aux questions suivantes en vous référant au scénario ci-dessus :

1. **Quel type de mesure de sécurité *EVEG* a-t-il mis en œuvre avec diligence pour se préparer aux perturbations et garantir que sa sécurité de l'information reste robuste et efficace, même dans des circonstances difficiles ?**
   A. Une mesure de sécurité technologique
   B. Une mesure de sécurité physique
   C. Une mesure de sécurité organisationnelle

2. ***EVEG* sera-t-il en mesure d'assurer la récupération après la perte de données ou de systèmes ?**
   A. Oui, parce qu'il a correctement mis en œuvre toutes les mesures de sécurité nécessaires
   B. Non, parce qu'elle n'a pas correctement mis en œuvre l'annexe A 8.13 sauvegarde *des renseignements* de l'annexe A
   C. Non, parce qu'elle n'a pas correctement mis en œuvre l'annexe A 5.29 *Sécurité de l'information pendant la perturbation* de l'annexe A

3. **Afin de réduire les risques de fraude, d'erreur et de contournement des mesures de sécurité de l'information, laquelle des mesures de sécurité**

suivantes a été mise en œuvre pour répartir les responsabilités au sein de l'entreprise ?

A. A 5.2 *Fonctions et responsabilités liées à la sécurité de l'information*
B. Annexe A 5.3 *Séparation des tâches*
C. Annexe A 5.4 *Responsabilités de la direction*

4. **Qu'est-ce que l'équipe SMSI a fait pour assurer la fiabilité et la récupérabilité de ses données et systèmes en cas de perturbations ?**

A. Il a établi une politique de sauvegarde
B. En effectuant des sauvegardes régulières
C. À la fois A et B

5. **En ne procédant pas à une analyse complète des coûts, qu'est-ce qu'*EVEG* n'a pas réussi à faire efficacement ?**

A. Préparer la mise en œuvre des mesures de sécurité
B. Concevoir et décrire les mesures de sécurité
C. Évaluer l'efficacité des mesures de sécurité

Quiz 22 : Surveillance, mesurage, analyse et évaluation

1. **Lors de la planification de la surveillance, du mesurage, de l'analyse et de l'évaluation, les organismes devraient définir leur « besoin en information », qui est une question ou une déclaration de haut niveau sur la sécurité de l'information qui aide l'organisme à évaluer le rendement en matière de sécurité de l'information, afin que ces évaluations répondent aux besoins définis en matière d'information.**
   A. Vrai
   B. Faux

2. **Qu'est-ce que la mesure ?**
   A. Processus d'observation d'un système, d'un processus ou d'un produit pour déterminer ses niveaux de performance
   B. Procédé de détermination de la valeur et des caractéristiques d'un système, d'un procédé ou d'un produit
   C. Processus d'examen d'un système, d'un processus ou d'un produit afin de mieux le comprendre

3. **Laquelle des déclarations suivantes concernant ISO/IEC 27004 est correcte ?**
   A. ISO/IEC 27004 fournit des lignes directrices pour aider les organismes à évaluer les performances du SMSI
   B. Les organismes peuvent obtenir une certification conformément à ISO/IEC 27004
   C. ISO/IEC 27004 ne précise PAS quoi et quand surveiller et mesurer

4. **Sur quel aspect les tableaux de bord stratégiques se concentrent-ils avant tout ?**
   A. Tâches opérationnelles détaillées et activités quotidiennes au sein de l'organisme
   B. Mesures de haut niveau des performances et prévisions pour les décideurs
   C. Évaluations individuelles du rendement des employés

5. **Selon ISO/IEC 27004, lequel des processus et activités ci-après ne fait PAS l'objet d'une mesure ?**
   A. Financement et gestion commerciale
   B. Communication et documentation
   C. Planification et audit

Quiz 23 : Audit interne

1. **Que fournit ISO 19011 ?**
   A. Exigences applicables aux organismes fournissant des services d'audit et de certification
   B. Lignes directrices concernant les compétences nécessaires que les auditeurs doivent posséder pour auditer un SMSI
   C. Conseils sur la gestion d'un programme d'audit et la planification et la réalisation d'audits de systèmes de gestion

2. **Qui est responsable de prendre les mesures requises et appropriées après la communication des résultats de l'audit ?**
   A. La direction générale
   B. Équipe d'audit
   C. Les consultants externes

3. **Les audits internes sont appelés audits par des tiers.**
   A. Vrai
   B. Faux

4. **Laquelle des déclarations suivantes concernant les audits internes n'est PAS correcte ?**
   A. Les audits internes n'ont pas de rôle consultatif au sein de l'organisme
   B. Les audits internes tiennent compte de l'efficacité et de l'efficience du SMSI
   C. Les audits internes sont indépendants des activités auditées

5. **Lequel des éléments suivants relève d'un auditeur interne ?**
   A. Planification des activités d'audit
   B. Établir l'étendue du programme d'audit
   C. Affectation des ressources nécessaires au programme d'audit interne

6. **Quelle est la définition correcte d'une non-conformité ?**
   A. Ne pas communiquer efficacement avec les parties prenantes
   B. Interruption temporaire des services en raison de la maintenance
   C. Non-satisfaction d'une exigence

7. **Les organismes doivent corriger toutes les non-conformités simultanément.**
   A. Vrai
   B. Faux

Quiz 24 : Revue de direction

1. **Un organisme qui souhaite se conformer à la norme ISO/IEC 27001 doit effectuer des examens de gestion aux intervalles prévus.**
   A. Vrai
   B. Faux

2. **Qui est chargé de veiller à ce que les plans d'action de suivi soient approuvés par la direction générale ?**
   A. Le coordinateur SMSI et l'équipe d'audit interne
   B. Le chef de projet SMSI
   C. Le responsable de la sécurité de l'information

3. **Lequel des éléments suivants n'a PAS besoin d'être inclus dans la revue de direction ?**
   A. Retour sur le rendement des employés
   B. Commentaires des parties intéressées
   C. Retour sur les performances en matière de sécurité de l'information

4. **Que faut-il inclure dans les extrants de la revue de direction, entre autres ?**
   A. Décisions relatives aux possibilités de traitement des risques
   B. Les décisions relatives aux possibilités d'amélioration continue
   C. À la fois A et B

5. **Selon ISO/IEC 27001, quelles informations doivent être documentées lors d'un examen de gestion ?**
   A. Résultats de la surveillance et des mesures
   B. Résultats de l'évaluation du risque
   C. À la fois A et B

Quiz 25 : Traitement des non-conformités

1. **Une mesure prise pour éliminer la cause d'une non-conformité et prévenir la récidive est connue sous le nom de :**
   A. Correction
   B. Action corrective
   C. Action préventive

2. **Selon la norme ISO/IEC 27001, qui est chargé de vérifier l'efficacité des mesures correctives prises en cas de non-conformité ?**
   A. L'organisme
   B. L'auditeur interne
   C. Le chef de projet SMSI

3. **Que doit inclure un plan d'action ?**
   A. Délai de mise en œuvre
   B. Les coûts des mesures correctives
   C. Les éléments de preuve de la non-conformité constatée

4. **Toutes les non-conformités devraient être incluses dans un seul plan d'action inclusif au lieu d'élaborer un plan d'action pour chaque non-conformité.**
   A. Vrai
   B. Faux

5. **Que se passe-t-il si le vérifié n'a pas présenté les plans d'action dans le délai imparti ?**
   A. Le vérifié devra demander une autre date de soumission
   B. L'auditeur émettra une non-conformité majeure
   C. L'audité ne sera pas recommandé pour la certification

6. **Quelles activités sont incluses dans la phase d'analyse de la situation du processus de mesures correctives, entre autres ?**
   A. Identification et documentation des non-conformités
   B. Suivi et revue des actions correctives
   C. Évaluation des options et sélection des solutions

Quiz 26 : Amélioration continue

1. **Lesquels des éléments suivants ne sont PAS considérés comme un facteur de changement du SMSI qui doit être surveillé ?**
   A. Changements dans les technologies
   B. Changements organisationnels
   C. Revues de produits

2. **De quoi dépend la fréquence d'examen du SMSI d'un organisme ?**
   A. Le nombre d'employés de l'organisme, ses revenus annuels et sa situation géographique
   B. Conformité de l'organisme aux règlements de l'industrie, aux commentaires des clients et à la satisfaction des employés
   C. La nature, l'envergure et la complexité de l'organisme, son profil de risque commercial et l'environnement dans lequel il exerce ses activités ;

3. **L'amélioration continue n'a aucun impact sur la collaboration entre les équipes.**
   A. Vrai
   B. Faux

4. **L'organisme A évalue et met à jour (au besoin) ses processus de SMSI chaque année pour s'assurer qu'ils sont efficaces. Une bonne pratique ?**
   A. Non, les processus du SMSI devraient être régulièrement évalués et mis à jour
   B. Oui, la norme ISO 27001 exige que les organismes évaluent et mettent à jour chaque année
   C. Non, les processus SMSI ne doivent être évalués et mis à jour que lorsque des non-conformités sont détectées

5. **Que fait-on lorsque les processus du SMSI et les mesures de sécurité de l'information sont compatibles avec les objectifs généraux, les activités et les processus de l'organisme ?**
   A. Pertinence
   B. Adéquation
   C. Efficacité

Quiz 27 : Préparation à l'audit de certification

1. **Au cours de quelle phase du processus de certification SMSI l'audit de l'étape 2 est-il mené ?**
   A. Avant l'audit
   B. Audit initial
   C. Après l'audit

2. **Laquelle des raisons suivantes n'est PAS valable pour rejeter un auditeur ?**
   A. L'auditeur a récemment vérifié un concurrent majeur du vérificateur
   B. L'auditeur a vérifié l'organisme par le passé
   C. L'auditeur a travaillé pour l'un des concurrents de l'organisme

3. **Quelle est l'activité principale de l'audit de l'étape 1 ?**
   A. Vérifier l'efficacité du système de management
   B. Examiner les informations documentées
   C. Évaluer la conformité aux exigences de la norme

4. **L'auditeur émet la décision finale de certification à la fin de l'audit.**
   A. Vrai
   B. Faux

5. **Quel est le but du suivi de l'audit ?**
   A. Valider le contrôle opérationnel des processus de l'auditeur
   B. Vérifier la « conception » du système de management
   C. Valider les plans d'action et les plans de mesures correctives présentés par l'entité auditée ;

Quiz 4 basé sur un scénario

Markt est une entreprise de recrutement réputée qui se spécialise dans la recherche d'employés qualifiés pour divers postes exigés par d'autres entreprises. L'entreprise opère dans un secteur concurrentiel où la nécessité de préserver la confidentialité, l'intégrité et la disponibilité des données des clients et des candidats est vitale. *Markt* traite les informations sensibles, y compris les données personnelles, les coordonnées et parfois même les données financières des candidats et des clients. Conscient de l'importance d'assurer la sécurité de l'information, *Markt* a décidé de mettre en place un système de gestion de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001. Suite à la mise en œuvre des exigences ISO/IEC 27001, *Markt* a décidé de procéder à un audit interne dans le cadre de l'évaluation des performances de son SMSI. La direction générale de l'entreprise a nommé Lisa en tant qu'auditeur interne pour planifier les dispositions d'un audit afin d'évaluer si le SMSI est conforme aux exigences de *Markt* pour le SMSI et aux exigences de la norme ISO/IEC 27001. Lisa s'est vu confier la responsabilité de déterminer les ressources requises pour le programme d'audit.

Lisa a établi les objectifs du programme d'audit et a procédé à la mise en œuvre des dispositions prévues. Elle n'a toutefois pas déterminé ni évalué les risques et les possibilités du programme d'audit puisqu'elle croyait que l'entreprise fonctionne dans un environnement à faible risque avec un minimum de changements dans ses processus ou sa réglementation. Afin d'assurer une évaluation complète du SMSI, Lisa a soigneusement planifié les principales activités conformément aux objectifs du programme d'audit. Ses activités d'audit prévues comprenaient l'examen de l'application par l'entreprise de politiques internes, de procédures et d'autres informations documentées pertinentes, de l'efficacité du processus d'exploitation et d'évaluation du risque de l'entreprise et du niveau de conformité aux lois, réglementations et exigences de la norme pertinente.

Après avoir recueilli suffisamment de preuves d'audit, Lisa les a évaluées en fonction des critères d'audit et a rédigé les constatations d'audit. Après avoir analysé et examiné les constatations en tenant compte des objectifs de l'audit, elle a publié les conclusions de l'audit, qui indiquaient à la fois les domaines de conformité et de non-conformité. Les non-conformités détectées par Lisa lors de l'audit ont été documentées dans un rapport de non-conformité. Après avoir reçu ce rapport, *Markt* a d'abord analysé la cause profonde des non-conformités identifiées, puis a sélectionné les mesures correctives appropriées pour y remédier.

Répondez aux questions suivantes en vous référant au scénario ci-dessus :

1. **La direction générale a confié à Lisa la responsabilité de déterminer les ressources nécessaires au programme d'audit. Est-ce conforme aux bonnes pratiques ?**
   A. Non, déterminer les ressources pour le programme d'audit relève du ministère des finances
   B. Non, déterminer les ressources pour le programme d'audit relève uniquement de la direction générale
   C. Oui, la personne qui gère le programme d'audit peut déterminer les ressources pour le programme d'audit

2. **Après avoir établi les objectifs du programme d'audit, Lisa a décidé de ne pas déterminer ni évaluer les risques et les possibilités du programme d'audit, car elle croyait que l'entreprise fonctionne dans un environnement à faible risque avec un minimum de changements dans ses processus ou sa réglementation. Est-ce conforme aux bonnes pratiques ?**
   A. Non, après avoir établi les objectifs du programme d'audit, il faudrait déterminer et évaluer les risques et les possibilités du programme d'audit.
   B. Oui, il n'est pas nécessaire d'évaluer les risques et les possibilités du programme d'audit si l'organisme fonctionne dans un environnement à faible risque avec un minimum de changements
   C. Non, le auditeur interne ne doit pas établir les objectifs du programme d'audit, car cette responsabilité relève de l'autorité de la direction générale.

3. **Afin d'assurer une évaluation complète du SMSI, Lisa a soigneusement planifié les principales activités conformément aux objectifs du programme d'audit. Laquelle des activités suivantes est considérée comme faisant partie des principales activités que Lisa aurait dû planifier entreprendre au cours de l'audit ?**
   A. Examen de l'affectation et de l'utilisation des ressources au sein de l'entreprise
   B. Enquête sur les plaintes des clients
   C. Examen de la gestion de la chaîne logistique de l'entreprise

4. **Après avoir reçu le rapport de non-conformité, *Markt a* d'abord analysé la cause première des non-conformités identifiées, puis a sélectionné les**

mesures correctives appropriées pour y remédier. Est-ce conforme aux bonnes pratiques ?

A. Non, les organismes devraient procéder à une analyse de situation avant de remédier à une non-conformité
B. Non, les organismes devraient analyser une ou plusieurs solutions possibles pour remédier aux non-conformités avant d'analyser leurs causes profondes
C. Oui, les organismes devraient analyser les causes profondes des non-conformités avant de déterminer les mesures correctives adéquates

5. **Lisa a-t-elle publié les conclusions de l'audit conformément aux pratiques exemplaires ?**

A. Oui, Lisa a publié les conclusions après avoir examiné les constatations de l'audit, en tenant compte des objectifs de l'audit
B. Non, Lisa aurait dû examiner les constatations de l'audit en collaboration avec le gestionnaire de projet SMSI de l'entreprise, puis publier les conclusions de l'audit
C. Non, Lisa aurait dû soumettre les constatations d'audit à la direction générale, qui peut ensuite rendre les conclusions d'audit