When Recognition Matters

Guide de préparation de l'examen

PECB Certified ISO/IEC 27001 Lead Auditor

L'objectif de l'examen « Certified ISO/IEC 27001 Lead Auditor » est de s'assurer que le candidat possède les connaissances et les compétences nécessaires pour planifier et réaliser un audit d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/IEC 27001 :2013, maîtriser les techniques et les principes d'audit, et pour gérer (ou de faire partie) des équipes d'audit et des programmes d'audit.

Les personnes ciblées pour cet examen sont :

- Les auditeurs qui souhaitent réaliser et diriger un audit d'un Système de Management de la Sécurité de l'Information (SMSI) comme responsable d'une équipe d'audit
- Les gestionnaires de projet ou les consultants qui souhaitent maîtriser le processus d'audit du Système de Management de la Sécurité de l'Information
- Les personnes responsables de la sécurité de l'information ou de la conformité dans une organisation
- Les membres d'une équipe de sécurité de l'information
- Les conseillers spécialisés en technologie de l'information
- Les experts techniques qui souhaitent se préparer à occuper une fonction d'audit de la sécurité de l'information

Le contenu de l'examen

- Domaine 1 : Principes et concepts fondamentaux de la sécurité de l'information (SI)
- Domaine 2 : Le Système de Management de la Sécurité de l'Information (SMSI)
- Domaine 3 : Principes et concepts fondamentaux d'audit
- Domaine 4 : Préparation d'un audit ISO/IEC 27001
- Domaine 5 : Conduire un audit ISO/IEC 27001
- Domaine 6 : Clôture d'un audit ISO/IEC 27001
- Domaine 7 : Gérer un programme d'audit ISO/IEC 27001

Le contenu de l'examen est divisé comme suit :

Domaine 1 : Principes et concepts fondamentaux de la sécurité de l'information (SI)

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et illustrer les concepts de la sécurité de l'information relatifs aux Système de Management de la Sécurité de l'Information (SMSI).

Compétences	Exposition des connaissances
1. Comprendre et expliquer les activités de l'organisation ISO et le développement des normes de la sécurité de l'information 2. Capacité à identifier, analyser et évaluer les exigences de conformité de la sécurité de l'information d'une organisation 3. Capacité à expliquer et illustrer les principaux concepts de la continuité d'activité et de la gestion des risques de la sécurité de l'information 4. Capacité à distinguer et expliquer la différence entre un actif de l'information, les données et les enregistrements 5. Comprendre, interpréter et illustrer la relation entre les concepts de l'actif, la vulnérabilité, la menace, l'impact et les contrôles	1. Connaissance de l'application des huit principes de l'ISO pour le management de la sécurité de l'information 2. Connaissance des principales normes de la sécurité de l'information 3. Connaissance des différentes sources des exigences de la sécurité de l'information d'une organisation : lois, règlements, normes internationales et de l'industrie, contrats, pratiques du marché, politiques internes. 4. Connaissances des principaux concepts de la sécurité de l'information et de la terminologie telle que décrite dans la norme ISO 27000 5. Connaissance de la notion du risque et de son application dans la sécurité de l'information 6. Connaissance de la relation entre les concepts d'actifs, de la vulnérabilité, de la menace, de l'impact et des contrôles 7. Connaissance de la différence et des caractéristiques des objectifs et des contrôles de sécurité 8. Connaissance de la différence entre la prévention, la détection et les contrôles correctifs et leurs caractéristiques

Domaine 2 : Le Système de Management de la Sécurité de l'Information (SMSI)

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et illustrer les concepts et les composants d'un Système de Management de la Sécurité de l'Information (SMSI), conforme à la norme ISO/IEC 27001.

Compétences	Exposition des connaissances
1. Comprendre et expliquer les composants d'un Système de Management de la	1. Connaissance des concepts, des principes et de la terminologie liés aux systèmes de management

Sécurité de l'Information conforme à la norme ISO/IEC 27001 et ses principaux processus 2. Capacité à interpréter et analyser les exigences de la norme ISO/IEC 27001 3. Comprendre, expliquer et illustrer les principales étapes pour établir, implémenter, faire fonctionner, surveiller, passer en revue, maintenir et améliorer un SMSI d'une organisation 4. Capacité à créer des objectifs de sécurité et à choisir les contrôles adaptés conformément à l'annexe A de la norme ISO/IEC 27001	et au modèle « Plan-Do-Check-Act » (PDCA) 2. Connaissance des principales caractéristiques d'un système de management intégré 3. Connaissance des principaux avantages d'une certification pour une organisation 4. Connaissance des exigences de la norme ISO/IEC 27001 présentées dans les clauses 4 à 8 5. Connaissance des principales étapes pour établir un SMSI et les politiques de sécurité, les objectifs de sécurité, les processus et les procédures relatives à la gestion du risque et à l'amélioration de la sécurité de l'information pour donner des résultats conformément à la politique et aux objectifs généraux de l'organisation (Niveau de sensibilisation) 6. Connaissance du concept d'amélioration continue et de son application dans un SMSI 7. Connaissance de la structure de l'Annexe A (objectifs et contrôles de sécurité)

Domaine 3 : Principes et concepts fondamentaux d'audit

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et appliquer les concepts et les principes relatifs à un audit du SMSI dans le contexte de la norme ISO/IEC 27001.

Compétences	Exposition des connaissances
1. Comprendre, expliquer et illustrer l'application des principes d'audit dans le contexte d'un audit ISO/IEC 27001. 2. Capacité à identifier et estimer les situations qui pourraient discréditer le professionnalisme d'un auditeur et du code d'éthique de PECB. 3. Capacité à identifier et évaluer les problèmes éthiques en prenant en compte les obligations relatives aux sponsors, à l'entité l'auditée et à l'application de la loi ou aux autorités règlementaires. 4. Capacité à expliquer, illustrer et appliquer l'approche d'audit basée sur les preuves dans le contexte d'un audit ISO/IEC 27001 5. Capacité à expliquer et comparer les types et les caractéristiques des preuves. 6. Capacité à déterminer et justifier quel type de preuve et combien de preuves sont requises dans le contexte d'une mission d'audit spécifique d'un SMSI. 7. Capacité à déterminer et évaluer le seuil de matérialité et appliquer l'approche basée sur le risque pendant les différentes phases d'un audit ISO/IEC 27001. 8. Capacité à juger le niveau approprié de	1. Connaissance des principaux concepts et de la terminologie, comme décrits par la norme ISO 19011 2. Connaissance des différences entre la première partie, la deuxième partie et la troisième partie de l'audit. 3. Connaissance des principes suivants d'audit : l'intégrité, la présentation équitable, la diligence professionnelle, le jugement professionnel, le scepticisme professionnel, la confidentialité et l'indépendance. 4. Connaissance de l'approche basée sur les preuves dans un audit. 5. Connaissance de la responsabilité professionnelle d'un auditeur et du code d'éthique de PECB. 6. Connaissance des différents types de preuves : physiques, mathématiques, confirmatives, techniques, analytiques, documentaires et verbales. 7. Connaissance de la qualité des preuves d'audit (admissibles, appropriées, fiables, et suffisantes) et les facteurs qui vont les influencer. 8. Connaissance de l'approche basée sur les risques dans un audit et des différents types de risques relatifs aux activités d'audit. 9. Connaissance du concept de matérialité et de son

l'assurance raisonnable nécessaire pour une mission spécifique d'audit ISO/IEC 27001.	application dans un audit. 10. Connaissance du concept d'assurance raisonnable et son application dans un audit.

Domaine 4 : Préparation d'un audit ISO/IEC 27001

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de préparer de manière appropriée un audit d'un SMSI dans le contexte de la norme ISO/IEC 27001.

Compétences	Exposition des connaissances
1. Comprendre et expliquer les étapes et les activités qu'il faut entreprendre pour préparer un audit d'un SMSI en prenant en compte le contexte spécifique et les conditions de la mission. 2. Comprendre et expliquer les rôles et les responsabilités d'un leader d'une équipe d'audit, des membres d'une équipe d'audit et des experts techniques. 3. Capacité à déterminer, évaluer et confirmer les objectifs d'audit, les critères d'audit et le domaine d'application de l'audit pour une mission spécifique d'audit ISO/IEC 27001. 4. Capacité à faire une étude de faisabilité d'un audit dans le contexte de la mission spécifique d'audit ISO/IEC 27001. 5. Capacité à expliquer, illustrer et définir les caractéristiques des notions d'audit et appliquer les meilleures pratiques pour établir le premier contact avec une entité auditée dans le contexte d'une mission spécifique d'audit ISO/IEC 27001. 6. Capacité à développer la documentation d'audit et à élaborer les plans appropriés de test d'audit dans le contexte d'une mission spécifique d'audit ISO/IEC 27001.	1. Connaissance des principales responsabilités d'un leader d'une équipe d'audit et des membres d'une équipe d'audit. 2. Connaissance des rôles et des responsabilités des expertes techniques d'un audit 3. Connaissance de la définition des objectifs d'audit, du domaine d'application de l'audit et des critères d'audit. 4. Connaissance de la différence entre le domaine d'application d'un SMSI et du domaine d'application de l'audit. 5. Connaissance des éléments à passer en revue pendant l'étude de faisabilité d'un audit. 6. Connaissance des aspects culturels à prendre en compte pendant un audit. 7. Connaissance des caractéristiques des notions d'audit et des meilleures pratiques pour établir un premier contact avec une entité auditée. 8. Connaissance de la préparation d'un plan d'audit 9. Connaissance de la préparation et de l'élaboration des documents nécessaires pour d'audit 10. Connaissance des avantages et des désavantages de l'utilisation des listes de contrôle de l'audit 11. Connaissance des meilleures pratiques pour la création d'une prolongation des plans de test

Domaine 5 : Conduire un audit ISO/IEC 27001

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de conduire de manière efficace un audit du SMSI dans le contexte de la norme ISO/IEC 27001.

Compétences	Exposition des connaissances
1. Capacité à organiser et conduire une	1. Connaissance des objectifs et du contenu d'une

réunion d'ouverture dans le contexte d'une mission spécifique d'audit ISO/IEC 27001. 2. Capacité à conduire une étape 1 de l'audit dans le contexte d'une mission spécifique d'audit ISO/IEC 27001 et prendre en compte les conditions et les critères de revue de la documentation 3. Capacité à conduire une étape 2 de l'audit dans le contexte d'une mission spécifique d'audit ISO/IEC 27001 en appliquant les meilleures pratiques de communication pour recueillir les preuves appropriées et prendre en compte les rôles et les responsabilités de toutes les personnes impliquées. 4. Capacité à expliquer, illustrer et appliquer les techniques statistiques et les méthodes d'échantillonnage d'audit. 5. Capacité à recueillir de manière objective les preuves appropriées de l'information disponible dans un audit et de les évaluer de manière objective.	réunion d'ouverture d'un audit. 2. Connaissance de la différence de l'étape 1 de l'audit et de l'étape 2 de l'audit. 3. Connaissance des exigences de l'étape 1 de l'audit, les étapes et les activités. 4. Connaissance des critères de la revue documentaire. 5. Connaissance des exigences documentaires énoncées par la norme ISO/IEC 27001. 6. Connaissances des exigences de l'étape 2 de l'audit, des étapes et des activités. 7. Connaissance des meilleures pratiques de communication pendant un audit. 8. Connaissance des rôles et des responsabilités des guides et des observateurs pendant un audit. 9. Connaissance des techniques de résolution de conflit. 10. Connaissance des procédures de recueil des preuves : observation, revue documentaire, entretiens, analyses et vérification technique. 11. Connaissance des procédures d'analyse des preuves : corroboration et évaluation. 12. Connaissance des concepts principaux, des principes et des techniques statistiques utilisées dans un audit. 13. Connaissance des méthodes principales d'échantillonnage d'audit et de leurs caractéristiques.

Domaine 6 : Clôture d'un audit ISO/IEC 27001

Objectifs principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de clôturer un audit d'un SMSI et de conduire des activités de suivi dans le contexte de la norme ISO/IEC 27001.

Compétences	Exposition des connaissances
1. Capacité à expliquer et appliquer les processus d'évaluation des preuves pour rédiger les résultats d'audit et préparer les conclusions d'audit. 2. Comprendre, expliquer et illustrer les différents niveaux de conformité et le concept du bénéfice du doute. 3. Capacité à faire un rapport des observations d'audit afin d'aider une organisation à améliorer un SMSI conformément aux principes et aux lois d'audit. 4. Capacité à compléter les documents d'un audit et à faire une revue de la qualité d'un audit ISO/IEC 27001 5. Capacité à rédiger des conclusions d'audit et les présenter à la direction de l'organisation auditée. 6. Capacité à organiser et conduire une réunion de clôture de l'audit.	1. Connaissance du processus d'évaluation des preuves pour rédiger les résultats d'audit et pour préparer les conclusions d'audit. 2. Connaissance des différences et des caractéristiques entre les concepts de conformité, de non-conformité mineure, de non-conformité majeure, de l'anomalie et de l'observation. 3. Connaissance des lignes directrices et des meilleures pratiques pour rédiger un rapport de non-conformité. 4. Connaissance des lignes directrices et des meilleures pratiques pour rédiger et faire le rapport de l'observation d'audit. 5. Connaissance du principe du bénéfice du doute et son application dans le contexte d'un audit. 6. Connaissance des lignes directrices et des meilleures pratiques pour compléter les documents d'un audit et pour faire une revue de la qualité d'un audit. 7. Connaissance des lignes directrices et des

7. Capacité à rédiger un rapport d'audit ISO/IEC 27001 et justifier une recommandation de certification 8. Capacité à conduire les activités suite à un audit initial incluant l'évaluation des plans d'actions, les audits de suivi, les audits de surveillance et les audits de recertification	meilleures pratiques pour présenter les résultats et les conclusions d'un audit à la direction d'une organisation auditée. 8. Connaissance des recommandations possibles qu'un auditeur peut donner dans le contexte d'un audit de certification et le processus de certification. 9. Connaissance des lignes directrices et des meilleures pratiques pour évaluer les plans d'actions. 10. Connaissance de l'audit de suivi, des audits de surveillance et des exigences d'un audit de recertification, des étapes et des activités. 11. Connaissance des conditions pour la modification, la prolongation, la suspension ou pour retirer la certification d'une organisation.

Domaine 7 : Gérer un programme d'audit ISO/IEC 27001

Objectif principal : S'assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre comment établir et gérer un programme d'audit d'un SMSI.

Compétences	Exposition des connaissances
1. Comprendre et expliquer l'établissement d'u programme d'audit et l'application du modèle PDCA. 2. Comprendre et expliquer la mise en œuvre d'un programme d'audit ISO/IEC 27001 (première partie, seconde partie et troisième partie) 3. Comprendre et expliquer les responsabilités pour protéger l'intégrité, la disponibilité et la confidentialité des enregistrements de l'audit. 4. Comprendre les exigences relatives aux composants du système de management d'un programme d'audit tel que la gestion de la qualité, la gestion des enregistrements, la gestion des plaintes 5. Comprendre l'évaluation de l'efficacité d'un programme d'audit en surveillant la performance de chaque auditeur, chaque équipe et de l'organisme de certification en général. 6. Comprendre et expliquer la façon dont les audits combinés sont traités dans un programme d'audit 7. Capacité à démontrer l'application des attributs personnels et les comportements associés aux auditeurs professionnels.	1. Connaissance de l'application du modèle PDCA dans la gestion d'un programme d'audit 2. Connaissance des exigences, des lignes directrices et des meilleures pratiques concernant les ressources, les procédures et les politiques d'audit 3. Connaissance des types d'outils utilisés par les auditeurs professionnels 4. Connaissances des exigences, des lignes directrices et des meilleures pratiques concernant la gestion des enregistrements d'audit 5. Connaissance de l'application du concept d'amélioration continue par la direction du programme d'audit 6. Connaissance des particularités pour mettre en œuvre et gérer une première partie, une seconde, ou troisième partie du programme d'audit. 7. Connaissance de la gestion des activités d'audit combiné 8. Connaissance du concept de compétence et son application aux auditeurs 9. Connaissance des attributs personnels et du comportement d'un auditeur professionnel.

Basé sur ces sept domaines et sur leur pertinence, l'examen contient douze questions, tel que résumé dans le tableau ci-dessous :

English	French
Level of Understanding (Cognitive/Taxonomy) Required	Niveau de compréhension requis (Cognitif/Taxonomie)
Points per question	Points par question
Questions that measure Comprehension, Application and Analysis	Question qui mesure la compréhension, l'application et l'analyse
Questions that measure Synthesis and Evaluation	Questions qui mesurent la synthèse et l'évaluation
Number of questions per content are	Nombre de question par domaine de compétence
% of test devoted to each content area	% du test consacré à chaque domaine de compétence
Content area/Competence domains	Domaines de compétences
Fundamental principles and concepts of IS	Principes et concepts fondamentaux de la SI
ISMS	SMSI
Fundamental audit concepts and principles	Principes et concepts fondamentaux d'audit
Preparation of an ISO 27001 audit	Préparation d'un audit ISO 27001
Conduct and ISO 27001 audit	Conduire un audit ISO 27001
Conclusion and follow-up of an ISO 27001 audit	Conclusion et suivi d'un audit ISO 27001
Managing an ISO 27001 audit program	Gérer un programme d'audit ISO 27001
Total points	Total des points
Number of questions per level of understanding	Nombre des questions par niveau de compréhension
% of test devoted to each level of understanding (cognitive/Taxonomy)	% du test consacré à chaque niveau de compréhension (cognitive/taxonomie)

Le score de passage est fixé à **70%.**

Après avoir réussi l'examen, les candidats peuvent demander la qualification de Certified ISO/IEC 27001 Lead Auditor en fonction de leur niveau d'expérience.

Passer l'examen de certification

Les candidats doivent arriver au moins trente (30) minutes avant le début de l'examen de certification. Les candidats qui arrivent en retard ne pourront pas bénéficier d'un délai supplémentaire pour compenser leur arrivée tardive et peuvent se voir refuser l'entrée à la salle d'examen (s'ils arrivent après plus de 5 minutes après le début de l'heure prévue de l'examen).

Tous les candidats devront présenter une carte d'identité valide avec une photo, comme un permis de conduire (ou toute autre pièce d'identité émise par le gouvernement) au surveillant et la lettre de confirmation de l'examen.

La durée de l'examen est de trois (3) heures.

Les questions sont des questions à développement. Ce type de format a été choisi car l'intention est de déterminer si un candidat est en mesure de rédiger une réponse cohérente, d'argumenter clairement et d'évaluer les techniques de résolution de problèmes. En raison de cette particularité, l'examen est défini comme à « livre ouvert » et ne mesure pas le rappel des données ou des informations. Au lieu de cela, l'examen évalue la compréhension, l'application, l'analyse, la synthèse et l'évaluation, ce qui signifie que même si la réponse est dans le matériel de cours, les candidats devront justifier et donner des explications, pour montrer qu'ils ont bien compris les concepts. A la fin de ce document, vous trouverez des échantillons de questions d'examen et des réponses possibles.

En étant un examen à "livre ouvert"; les candidats sont autorisés à utiliser les documents de référence ci-dessous :

- Une copie de la norme ISO/IEC 27001 :2013
- Le manuel de cours du participant,
- Toutes les notes personnelles prises par le participant durant le cours et
- Un dictionnaire.

L'utilisation d'appareils électroniques, comme les ordinateurs portables ou les téléphones portables, n'est pas autorisée.

Toute tentative de copier, de s'associer avec quelqu'un ou de tricher pendant l'examen conduira automatiquement à l'échec de l'examen.

Les examens de PECB sont disponibles en anglais. Pour savoir si l'examen est disponible dans une autre langue, veuillez nous contacter à l'adresse : examination@pecb.com

Réception des résultants de l'examen

Les résultats seront communiqués par courrier électronique dans un délai de 6 à 8 semaines suivant l'examen. Les résultats ne dévoileront pas la note exacte que le candidat a obtenue, mais seulement une mention de réussite ou d'échec.

Les candidats qui auront réussi l'examen seront en mesure de postuler au schéma de certification.

En cas d'échec, les résultants seront accompagnés de la liste des domaines dans lesquels le candidat a obtenu une mauvaise note, pour donner une orientation qui l'aidera dans la préparation pour passer de nouveau l'examen.

Les candidats qui sont en désaccord avec les résultats de l'examen peuvent déposer une plainte. Pour plus d'informations, veuillez visiter : www.pecb.com

Politique de passage de l'examen

Il n'y a aucune limitation sur le nombre de fois qu'un candidat peut passer le même examen. Cependant, il existe certaines limites en termes de calendrier entre les deux examens.

Lorsque les candidats échouent à un examen, ils sont autorisés à reprendre l'examen une fois dans les 12 mois après la première tentative. Si le deuxième examen est un échec, le candidat peut passer l'examen seulement après une année (12 mois). Des frais de reprise s'appliquent.

Seuls les étudiants qui ont complété une formation entière du PECB mais qui échouent à l'examen écrit, son admissibles à l'examen sans frais, à condition que :

"Un étudiant peut repasser l'examen une fois et cette reprise doit avoir lieu dans les 12 mois à compter de la date de l'examen initial. »

Lorsque les candidats échouent au même examen pour la seconde fois, leur dossier est automatiquement fermé pour une année.

Fermeture des dossiers

La fermeture d'un dossier est équivalente au rejet de la demande d'un candidat. En conséquence, lorsque les candidats demandent que leur dossier soit rouvert, PECB ne sera plus lié aux conditions, aux normes, aux politiques, au manuel du candidat ou au guide de préparation de l'examen qui était en vigueur avant que leur dossier n'ait été fermé.

Les candidats qui souhaitent demander la réouverture de leur dossier doivent faire une demande écrite et payer les frais requis.

Sécurité de l'examen

L'élément important d'une certification professionnelle réussie est le respect et le maintien de la sécurité et de la confidentialité de l'examen. PECB compte sur le comportement éthique des détenteurs des certificats et des candidats pour maintenir la sécurité et la confidentialité de ses examens. Lorsque quelqu'un qui détient une qualification de PECB révèle des informations sur le contenu de l'examen, il viole le code d'éthique de PECB. PECB prendra des mesures contre les personnes qui enfreignent ses conditions et son code d'éthique. Les mesures prises peuvent inclure l'interdiction permanente des individus à poursuivre les qualifications de PECB et peut révoquer les certifications de ceux qui ont obtenu le diplôme. PECB entamera également une action en justice contre les personnes ou les organisations qui portent atteinte à ses droits d'auteur, aux droits de propriété et à la propriété intellectuelle.

Exemples de questions d'examen et réponses possibles

1. Preuves dans un audit

Déterminez de quelle façon vérifierez chacune des mesures de contrôle ci-après. Vous devez fournir des exemples de preuves que vous souhaitez rechercher pour avoir une garantie raisonnable que la mesure de contrôle a été mise en œuvre de manière efficace. Veuillez indiquer aux moins deux éléments de preuves pour chaque mesure.

Les politiques de la sécurité de l'information (A.5.1.1.) :

Réponses possibles :

- Revue documentaire de la politique de la sécurité de l'information pour valider le contenu
- Entretien avec la personne chargée de la sécurité de l'information pour valider le processus d'approbation et de distribution de la politique.
- Vérification des moyens de distribution de la politique (site internet, version imprimée, information sur le manuel de l'employée, etc.)

2. Evaluation des actions correctives

Vous avez reçu un plan d'actions correctives. Evaluez l'adéquation des actions correctives proposées. Si vous êtes d'accord avec les actions correctives, expliquez pourquoi. Si vous n'êtes pas d'accord, expliquez pourquoi et proposez quelles seraient les actions correctives adéquates.

- Une non-conformité a été observée car l'équipe des ressources humaines n'était pas au courant de la procédure qui leur demande de valider les références des futurs employés avant de les embaucher.
- L'action corrective : informer (délai d'exécution : immédiat) et former (délai d'exécution : dans les 6 mois) l'équipe des ressources humaines concernant cette procédure et demander que chaque membre de l'équipe suive la formation.

  Réponses possibles
  Je suis d'accord. Ceci résout le problème qui était l'ignorance de la procédure. En tant qu'auditeur, un échantillonnage sera réalisé pendant l'audit de surveillance pour vérifier si la procédure est suivie.

3. Evaluation du risque et sélection des contrôles

   Déterminer les menaces et les vulnérabilités associées aux situations suivantes et indiquer les impacts potentiels. Indiquer, également, si les risques affecteraient la confidentialité, l'intégrité des données et/ou la disponibilité.

Pour chaque risque identifié, fournir les contrôles appropriés (en fournissant le numéro de la clause de la mesure) qui permet de réduire, de transférer ou d'éviter les risques.

Réponses possibles :

Enoncé	Vulnérabilités	Menaces	C	I	A	Impacts potentiels	Contrôles
Le webmestre qui a créé le site internet de l'entreprise et il est chargé des mises à jour et de télécharger les informations sur le site	Manque de ségrégation des fonctions Une personne seulement est disponible pour cette fonction	Erreurs de traitement Actes malveillants Le webmestre démissionne de l'entreprise ou tombe malade		X	X	Le site internet contant des informations erronées : perte de crédibilité Site internet non disponible : perte de revenus	A.12.1.1 A.6.1.2 A.9.2.3 A.14.1.2 A.12.4.3 A.14.2.2

4. Classification des mesures

Pour chacun des 5 mesures suivantes, indiquez si elle a été utilisée comme une mesure préventive, corrective, et/ou de détection ; et indiquez si la mesure est une mesure administrative, technique, managériale ou légale. Expliquez votre réponse.

- Le cryptage des communications électroniques

Réponses possibles :

Mesure préventive : empêche les personnes non-autorisées de lire les messages

Mesures techniques (peuvent être légales) : le cryptage est une solution technique pour assurer la confidentialité de l'information (peut être une exigence légale)

5. Rédaction d'un plan de test

Rédigez un plan de test pour valider la mesure suivante, qui identifie les différentes procédures applicables d'audit (observation, revue documentaire, entretien, vérification technique et analyse) :

- Protection de l'information journalisée (A.12.4.2). Les appareils de connexion et les informations de connexion doivent être protégés contre les falsifications et l'accès non-autorisé.

Réponses possibles :

Protection des informations journalisées (A.12.4.2) : les appareils de connexion et les informations de connexion doivent être protégés contre la falsification et l'accès non-autorisé.	
Observation	Observation des mesures de protection mises en œuvre contre le sabotage et les accès non-autorisés.
Documentation	La documentation des mesures en place pour protéger l'information journalisée contre le sabotage et les accès non-autorisés, la politique de l'information journalisée et les procédures afférentes, les rapports de test d'intrusion.
Entretien	Entretien avec le gestionnaire de la sécurité de l'information et valider les objectifs de la politique de journalisation, entretien avec l'administrateur de réseau pour valider le fonctionnement des mesures en place pour protéger l'information journalisée contre le sabotage et les accès non-autorisés.
Vérification technique	Observation des configurations de l'équipement de journalisation pour vérifier leur conformité aux politiques et aux procédures de l'organisation.
Analyse	Analyse d'un échantillon d'information journalisée.