PECB BEYOND RECOGNITION

Manuel du candidat

ISO/IEC 27001 LEAD IMPLEMENTER

PECB

Table des matières

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui propose des services d'éducation[1] et de certification de personnes selon la norme ISO/IEC 17024, dans un large éventail de disciplines.

Nous aidons les professionnels à faire preuve d'engagement et de compétence en leur fournissant des services d'évaluation et de certification en fonction de normes reconnues internationalement. Notre mission est de fournir des services qui inspirent la confiance, l'amélioration continue, assurent la reconnaissance et profitent à la société dans son ensemble.

Les principaux objectifs de PECB sont les suivants :

1. Établir les exigences minimales nécessaires pour certifier les professionnels
2. Examiner et vérifier les qualifications des candidats pour s'assurer qu'ils sont éligibles à la certification
3. Développer et maintenir des évaluations de certification fiables
4. Délivrer des certifications aux candidats qualifiés, tenir des registres et publier un répertoire des détenteurs de certifications valides
5. Établir les exigences pour le renouvellement périodique de la certification et veiller au respect de ces exigences
6. S'assurer que les candidats respectent les normes éthiques dans leur pratique professionnelle
7. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification auprès des organisations, des employeurs, des fonctionnaires, des praticiens dans des domaines connexes et auprès du public

[1] Éducation fait référence aux formations développées par PECB, et offertes dans le monde entier par le biais de notre réseau de partenaires.

Valeur de la certification PECB

Pourquoi choisir PECB en tant qu'organisme de certification ?

Reconnaissance mondiale

Nos certifications sont reconnues à l'échelle internationale et accréditées par l'IAS (International Accreditation Service), signataire du Multilateral Recognition Arrangement (MLA) de l'IAF qui assure la reconnaissance mutuelle de la certification accréditée entre les signataires du MLA et l'acceptation de la certification accréditée dans de nombreux marchés. Par conséquent, les professionnels qui obtiennent un titre de certification de PECB bénéficieront de la reconnaissance de PECB sur les marchés nationaux et internationaux.

Personnel compétent

L'équipe centrale de PECB est composée de personnes compétentes qui possèdent une expérience pertinente des différents domaines. Tous nos employés détiennent des titres professionnels et sont constamment formés pour fournir des services plus que satisfaisants à nos clients.

Conformité aux normes

Nos certifications sont une démonstration de la conformité à la norme ISO/IEC 17024. Elles garantissent que les exigences de la norme ont été remplies et validées avec la cohérence, le professionnalisme et l'impartialité adéquats.

Service client

Nous sommes une entreprise centrée sur le client et nous traitons tous nos clients avec estime, importance, professionnalisme et équité. PECB dispose d'une équipe d'experts qui se consacrent au soutien des demandes, problèmes, préoccupations, besoins et opinions des clients. Nous faisons de notre mieux pour maintenir un temps de réponse maximum de 24 heures sans compromettre la qualité du service.

Code de déontologie de PECB

Les professionnels de PECB sont tenus de :

1. Se comporter de manière professionnelle, avec honnêteté, exactitude, équité, responsabilité et indépendance
2. Agir en tout temps uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, en respectant les normes professionnelles et les techniques applicables tout en offrant des services professionnels
3. Maintenir leurs compétences dans leurs domaines respectifs et s'efforcer d'améliorer constamment leurs capacités professionnelles
4. Ne proposer que des services professionnels pour lesquels ils sont qualifiés et informer correctement les clients de la nature des services proposés, y compris de toute préoccupation ou risque pertinent
5. Informer chaque employeur ou client de tout intérêt commercial ou affiliation qui pourrait influencer leur jugement ou nuire à leur équité
6. Traiter de manière confidentielle et privée les informations obtenues dans le cadre des relations professionnelles et commerciales de tout employeur ou client, actuel ou ancien
7. Se conformer à toutes les lois et réglementations des juridictions dans lesquelles les activités professionnelles sont exercées
8. Respecter la propriété intellectuelle et la contribution d'autrui
9. Ne pas communiquer, intentionnellement ou non, des informations fausses ou falsifiées qui pourraient compromettre l'intégrité du processus d'évaluation d'un candidat à un titre professionnel
10. Ne pas agir d'une manière qui pourrait compromettre la réputation de PECB ou de ses programmes de certification
11. Coopérer pleinement à l'enquête qui suit une violation présumée du présent
12. Code de déontologie. La version complète du Code de déontologie de PECB peut être téléchargée ici.

Introduction à ISO/IEC 27001 Lead Implementer

ISO/IEC 27001 a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information (SMSI). Les compétences les plus importantes requises sur le marché sont la capacité à planifier, à mettre en œuvre et à gérer efficacement le SMSI, à évaluer et à traiter les risques liés à la sécurité de l'information, à sélectionner et à mettre en œuvre les mesures de sécurité de l'information, et à gérer (ou faire partie) des équipes de mise en œuvre du SMSI.

Le titre de compétence « ISO/IEC 27001 Lead Implementer » est une certification professionnelle destinée aux personnes qui souhaitent démontrer leur compétence à mettre en œuvre un système de management de la sécurité de l'information et à diriger une équipe de mise en œuvre du SMSI.

La mise en œuvre étant l'une des professions les plus demandées, une certification reconnue au niveau international peut vous aider à exploiter votre potentiel de carrière et à atteindre vos objectifs professionnels.

Il est important de préciser que les certifications de PECB ne sont pas une licence ou une simple adhésion. Il s'agit d'une reconnaissance par les pairs qu'une personne a démontré sa maîtrise et sa compréhension d'un ensemble de compétences. Les certifications PECB sont accordées aux candidats qui peuvent fournir la preuve de leur expérience et qui ont réussi un examen normalisé dans le domaine de la certification.

Le présent document spécifie le programme de certification PECB ISO/IEC 27001 Lead Implementer conformément à la norme ISO/IEC 17024:2012. Il contient également des informations sur le processus par lequel les candidats peuvent obtenir et renouveler leur certification. Il est très important que vous lisiez toutes les informations contenues dans ce manuel avant de remplir et de soumettre votre candidature. Si vous avez des questions après la lecture de ce document, veuillez contacter le bureau international de PECB à certification.team@pecb.com.

SECTION II : PROCESSUS DE CERTIFICATION ET PRÉPARATION, RÈGLES ET POLITIQUES RELATIFS À L'EXAMEN DE PECB

Décidez de la certification qui vous convient

Toutes les certifications PECB ont des exigences spécifiques en matière de formation et d'expérience professionnelle. Pour déterminer le titre de compétence qui vous convient, vérifiez les critères d'admissibilité des diverses certifications et vos besoins professionnels.

Préparer et programmer l'examen

Les candidats sont responsables de leur propre étude et de leur préparation aux examens de certification. Aucun ensemble spécifique de cours ou de programmes d'études n'est requis dans le cadre du processus de certification. Toutefois, la participation à une session de formation peut augmenter de manière significative les chances de réussite à l'examen PECB.

Pour programmer un examen de certification PECB, les candidats ont deux options :

1. Contacter l'un de nos partenaires qui proposent des sessions de formation et d'examen. Les candidats trouveront un partenaire de formation dans une région donnée sur la page Liste des partenaires. Le calendrier des sessions de formation PECB est également disponible sous l'onglet Calendrier des formations.
2. Passer un examen PECB à distance de chez eux ou de n'importe quel endroit qu'ils préfèrent grâce à l'application PECB Exams, qui est accessible ici : Sessions d'examens.

Pour en savoir plus sur les examens, les domaines de compétences et les énoncés de connaissances, veuillez vous référer à la *section III* du présent document.

Frais de demande d'examen et de certification

PECB propose aussi les examens directement, où un candidat peut se présenter à l'examen sans assister à la formation. Les prix sont les suivants :

- Examen Lead : 1000 $ US
- Examen Manager : 700 $ US
- Examens Foundation et Transition :

Les frais de demande de certification sont de 500 $ US.

Pour tous les candidats qui ont suivi la formation et passé l'examen auprès d'un partenaire PECB, le coût de la session de formation comprend les frais associés à l'examen (examen et première reprise) et à la demande de certification, ainsi que la première année de frais annuels de maintenance (FAM).

Domaines de compétence

L'examen « PECB ISO/IEC 27001 Lead Implementer » a pour objectif de veiller à ce que le candidat ait acquis les compétences nécessaires pour soutenir une organisation dans l'établissement, la mise en œuvre, la gestion et le maintien du système de management de la sécurité de l'information (SMSI) basé sur les exigences d'ISO/IEC 27001.

La certification ISO/IEC 27001 Lead Implementer est destinée aux :

- Responsables de projet ou consultants souhaitant préparer et soutenir une organisation dans la mise en œuvre d'un système de management de la sécurité de l'information dans une organisation
- Chefs de projet, consultants ou conseillers experts cherchant à maîtriser la mise en œuvre d'un SMSI
- Personnes responsables du maintien de la conformité aux exigences d'ISO/IEC 27001 dans une organisation
- Membres d'une équipe de mise en œuvre d'un SMSI

L'examen couvre les domaines de compétence suivants :

- **Domaine 1 :** Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)
- **Domaine 2 :** Système de management de la sécurité de l'information (SMSI)
- **Domaine 3 :** Planification de la mise en œuvre d'un SMSI selon ISO/IEC 27001
- **Domaine 4 :** Mise en œuvre d'un SMSI selon ISO/IEC 27001
- **Domaine 5 :** Surveillance et mesure d'un SMSI selon ISO/IEC 27001
- **Domaine 6 :** Amélioration continue d'un SMSI selon ISO/IEC 27001
- **Domaine 7 :** Préparation à un audit de certification du SMSI

PECB

Domaine 1 : Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)

Objectif principal : S'assurer que le candidat comprend et est capable d'interpréter les principes et les concepts de la norme ISO/IEC 27001

Compétences	Énoncés de connaissances
1. Comprendre et expliquer les principaux concepts de la sécurité de l'information 2. Expliquer la différence et la relation entre l'information et l'actif 3. Comprendre la différence entre les documents, les spécifications et les enregistrements 4. Comprendre la relation entre les concepts de vulnérabilité, de menace, de risque et leur impact 5. Comprendre les concepts de confidentialité, d'intégrité et de disponibilité des informations 6. Comprendre et interpréter la classification des mesures de sécurité et leurs objectifs 7. Capacité à comprendre la relation entre les éléments de sécurité de l'information.	1. Connaissance des lois, règlements, normes internationales et industrielles, contrats, pratiques du marché, politiques internes, bonnes pratiques, etc. en matière de sécurité de l'information auxquels une organisation doit se conformer 2. Connaissance des principaux concepts et de la terminologie de la norme ISO/IEC 27001 3. Connaissance du risque de sécurité de l'information et de son importance dans un SMSI 4. Connaissance de la confidentialité, de l'intégrité et de la disponibilité des informations 5. Connaissance des vulnérabilités, menaces et risques liés à la sécurité de l'information 6. Connaissance des impacts potentiels qui peuvent affecter la confidentialité, l'intégrité ou la disponibilité des informations 7. Connaissance de la différence entre les types de mesures de sécurité tels que les mesures techniques, juridiques, administratives et de management. 8. Connaissance de la différence entre les mesures de sécurité classées selon leur fonction, telles que les mesures préventives, correctives et de détection.

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

Objectif principal : S'assurer que le candidat comprend et est capable de mettre en œuvre les mesures de sécurité énumérés dans l'annexe A de la norme ISO/IEC 27001

Compétences	Énoncés de connaissances
1. Sélectionner, concevoir et décrire les mesures de sécurité de l'information 2. Définir l'architecture de sécurité de l'organisation 3. Identifier et illustrer les activités liées au développement et au déploiement des systèmes d'information 4. Documenter la mise en œuvre des mesures de sécurité de l'information sélectionnées 5. Comprendre, interpréter et analyser les mesures de l'annexe A de la norme ISO/IEC 27001 6. Mettre en œuvre les mesures de sécurité de l'annexe A sur la base d'ISO/IEC 27001 et des bonnes pratiques	1. Connaissance des services de sécurité courants tels que les services de contrôle d'accès, les services de contrôle des frontières, les services d'intégrité, les services cryptographiques et les services d'audit et de surveillance. 2. Connaissance des cadres d'architecture les plus courants 3. Connaissance des 93 mesures de l'Annexe A de la norme ISO/IEC 27001 4. Connaissance des quatre groupes de mesures de l'Annexe A, à savoir les contrôles organisationnels, les contrôles des personnes, les contrôles physiques et les contrôles technologiques. 5. Connaissance de la sélection et de la mise en œuvre des mesures de l'Annexe A d'ISO/IEC 27001 6. Connaissance de la documentation des mesures de sécurité de l'information sélectionnées.

PECB

Domaine 3 : Planification de la mise en œuvre d'un SMSI selon ISO/IEC 27001

Objectif principal : S'assurer que le candidat est capable de planifier la mise en œuvre du SMSI basé sur la norme ISO/IEC 27001

Compétences

1. Recueillir, analyser et interpréter les informations nécessaires à la planification de la mise en œuvre d'un SMSI
2. Comprendre et fixer les objectifs de la sécurité de l'information et du SMSI
3. Identifier et interpréter les risques liés au SMSI et leurs impacts
4. Analyser et prendre en compte le contexte interne et externe d'une organisation
5. Identifier les ressources nécessaires à la mise en œuvre du SMSI
6. Gérer, estimer et contrôler les ressources nécessaires à la mise en œuvre du SMSI
7. Identifier les rôles et responsabilités des principales parties intéressées pendant et après la mise en œuvre et l'exploitation d'un SMSI
8. Rédiger, classer et réviser un plan de projet SMSI
9. Effectuer une analyse des écarts et clarifier les objectifs de management de la sécurité de l'information
10. Définir et justifier un périmètre SMSI adapté aux objectifs spécifiques de sécurité de l'information de l'organisation
11. Développer et établir une politique SMSI
12. Effectuer les différentes étapes du processus d'appréciation des risques
13. Comprendre et rédiger la Déclaration d'applicabilité

Énoncés de connaissances

1. Connaissance des principaux concepts, de la terminologie, des processus et des meilleures pratiques en matière de gestion de projet
2. Connaissance des principales approches et méthodologies utilisées pour mettre en œuvre un SMSI
3. Connaissance des objectifs typiques de la sécurité de l'information et du SMSI et de la manière d'atteindre des résultats spécifiques
4. Connaissance de ce qui constitue typiquement le contexte interne et externe d'une organisation
5. Connaissance des approches utilisées pour comprendre le contexte d'une organisation
6. Connaissance des techniques utilisées pour recueillir des informations sur une organisation et pour effectuer une analyse des écarts d'un système de management
7. Connaissance d'un plan de projet SMSI et d'une équipe de projet SMSI
8. Connaissance des ressources nécessaires à la mise en œuvre d'un SMSI
9. Connaissance des principales structures organisationnelles applicables à une organisation pour gérer un SMSI
10. Connaissance des caractéristiques du périmètre d'un SMSI en termes de limites organisationnelles, technologiques et physiques
11. Connaissance des bonnes pratiques et techniques utilisées pour rédiger et établir des politiques et procédures de sécurité de l'information
12. Connaissance des différentes approches et méthodologies utilisées pour réaliser le processus d'appréciation des risques
13. Connaissance des caractéristiques de la Déclaration d'applicabilité

PECB

Domaine 4 : Mise en œuvre d'un SMSI selon ISO/IEC 27001

Objectif principal : S'assurer que le candidat est capable de mettre en œuvre un SMSI basé sur les exigences de la norme ISO/IEC 27001

Compétences	Énoncés de connaissances
1. Gérer les processus de renforcement des capacités pour la mise en œuvre réussie d'un SMSI	1. Connaissance des bonnes pratiques en matière de gestion du cycle de vie des informations documentées
2. Définir les processus de documentation et de gestion des enregistrements nécessaires pour soutenir la mise en œuvre et le fonctionnement d'un SMSI	2. Connaissance des caractéristiques et des différences entre les différentes informations documentées liées à une politique, une procédure, une ligne directrice, une norme, une ligne de base, une feuille de travail du SMSI, etc.
3. Définir, concevoir et mettre en œuvre les processus nécessaires au fonctionnement d'un SMSI et les documenter correctement	3. Connaissance des trois V du big data : volume, variété et vélocité
4. Comprendre, gérer et évaluer les connaissances organisationnelles	4. Connaissance de l'intelligence artificielle faible et forte, et de l'apprentissage automatique
5. Comprendre les tendances et les technologies du monde actuel telles que le big data, l'intelligence artificielle, l'apprentissage automatique, le cloud computing et les opérations externalisées	5. Connaissance des services de cloud computing : infrastructure en tant que service (IaaS), plateforme en tant que service (PaaS) et logiciel en tant que service (SaaS)
6. Définir et mettre en œuvre des programmes appropriés de formation et de sensibilisation à la sécurité de l'information, ainsi que des plans de communication	6. Connaissance de l'impact des nouvelles technologies dans la sécurité de l'information
7. Établir un plan de communication du SMSI afin d'aider à la compréhension des problèmes, des politiques et des performances de l'organisation en matière de sécurité de l'information, et de fournir des informations ou des suggestions pour améliorer les performances du SMSI	7. Connaissance des caractéristiques et des bonnes pratiques pour mener des plans de formation, de sensibilisation et de communication en matière de management du risque
8. Mettre en place une politique de gestion des incidents et une équipe de réponse aux incidents	8. Connaissance des caractéristiques et des bonnes pratiques de mise en œuvre de programmes de formation et de sensibilisation à la sécurité de l'information et de plans de communication
9. Comprendre la différence entre la continuité d'activité et la reprise après sinistre	9. Connaissance de la continuité d'activité et de la reprise après sinistre
	10. Continuité d'activité et reprise d'activité après sinistre

PECB

Domaine 5 : Surveillance et mesure d'un SMSI selon ISO/IEC 27001

Objectif principal : S'assurer que le candidat est capable d'analyser, d'évaluer, de surveiller et de mesurer les performances d'un SMSI

Compétences	Énoncés de connaissances
1. Surveiller et évaluer l'efficacité d'un SMSI 2. Vérifier dans quelle mesure les objectifs identifiés du SMSI ont été atteints 3. Définir et mettre en œuvre un programme d'audit interne du SMSI 4. Effectuer des revues régulières et méthodiques pour s'assurer de la pertinence, de l'adéquation, de l'efficacité et de l'efficience d'un SMSI basé sur les politiques et les objectifs de l'organisation 5. Définir et mettre en œuvre un processus de revue de direction	1. Connaissance des bonnes pratiques et des techniques utilisées pour surveiller et évaluer l'efficacité d'un SMSI 2. Connaissance des concepts liés à la mesure et à l'évaluation 3. Connaissance des principaux concepts et éléments liés à la mise en œuvre et au fonctionnement d'un programme d'audit interne du SMSI 4. Connaissance de la différence entre une non-conformité majeure et une non-conformité mineure 5. Connaissance des lignes directrices et des bonnes pratiques pour rédiger un rapport de non-conformité 6. Connaissance des bonnes pratiques utilisées pour effectuer des revues de direction

PECB

Domaine 6 : Amélioration continue d'un SMSI selon ISO/IEC 27001 **Objectif principal :** S'assurer que le candidat est capable de fournir des conseils sur l'amélioration continue d'un SMSI	
Compétences	**Énoncés de connaissances**
1. Suivre et prendre des mesures concernant les non-conformités 2. Identifier et analyser les causes profondes des non-conformités, et proposer des plans d'action pour les traiter 3. Conseiller une organisation sur la manière d'améliorer continuellement l'efficacité et l'efficience d'un SMSI 4. Mettre en œuvre des processus d'amélioration continue dans une organisation 5. Déterminer les outils appropriés pour soutenir les processus d'amélioration continue d'une organisation	1. Connaissance des principaux processus, outils et techniques utilisés pour identifier les causes profondes des non-conformités 2. Connaissance du processus de traitement des non-conformités 3. Connaissance des principaux processus, outils et techniques utilisés pour élaborer des plans d'action corrective 4. Connaissance des principaux concepts liés à l'amélioration continue 5. Connaissance des processus liés à la surveillance continue des facteurs de changement 6. Connaissance du maintien et de l'amélioration d'un SMSI

PECB

Domaine 7 : Préparation à un audit de certification du SMSI

Objectif principal : S'assurer que le candidat ISO/IEC 27001 Lead Implementer est capable de préparer une organisation à la certification ISO/IEC 27001

Compétences	Énoncés de connaissances
1. Comprendre les principales étapes, processus et activités liées à l'audit de certification ISO/IEC 27001 2. Comprendre, expliquer et illustrer l'approche des preuves d'audit dans un audit du SMSI 3. Conseiller une organisation pour identifier et sélectionner un organisme de certification qui répond à ses attentes 4. Déterminer si une organisation est prête et préparée pour l'audit de certification ISO/IEC 27001 5. Former et préparer le personnel d'une organisation à l'audit de certification ISO/IEC 27001 6. Argumenter et contester les résultats et les conclusions de l'audit avec les auditeurs externes	1. Connaissance de l'approche d'un audit basée sur les preuves 2. Connaissance des types d'audit et de leurs différences 3. Connaissance des différences entre les audits de phase 1 et de phase 2 4. Connaissance des exigences, des étapes et des activités de l'audit de phase 1 5. Connaissance des critères de révision des informations documentées 6. Connaissance des exigences, des étapes et des activités de l'audit de phase 2 7. Connaissance des exigences, des étapes et des activités de suivi d'audit 8. Connaissance des exigences, des étapes et des activités des audits de surveillance et des audits de renouvellement 9. Connaissance des exigences, des lignes directrices et des bonnes pratiques pour l'élaboration de plans d'action à la suite d'un audit de certification ISO/IEC 27001

Sur la base de ces domaines et de leur pertinence, 80 questions sont incluses dans l'examen, comme résumé dans le tableau ci-dessous :

				Niveau de compréhension (Cognitif/Taxonomique) requis	
		Nombre de questions/ points par domaine de compétence	%/points de l'examen consacré à chaque domaine de compétence	Questions qui mesurent la compréhension, l'application et l'analyse	Questions qui mesurent la synthèse et l'évaluation
Domaines de compétence	Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)	15	18,75	X	
	Système de management de la sécurité de l'information (SMSI)	12	15	X	
	Planification de la mise en œuvre du SMSI selon ISO/IEC 27001	18	22,5		X
	Mise en œuvre du SMSI selon ISO/IEC 27001	14	17,5		X
	Surveillance et mesure du SMSI selon ISO/IEC 27001	10	12,5	X	
	Amélioration continue du SMSI selon ISO/IEC 27001 ISO/IEC 27001	6	7,5	X	
	Préparation à un audit de certification du SMSI	5	6,25		X
	Total des points	**80**	**100 %**		
	Nombre de questions par niveau de compréhension			**43**	**37**
	Pourcentage de l'examen consacré à chaque niveau de compréhension (cognitif/taxonomie)			**53.75 %**	**46.25 %**

La note de passage est établie à **70 %**.

Après avoir réussi l'examen, les candidats pourront demander la certification « PECB Certified ISO/IEC 27001 Lead Implementer » en fonction de leur niveau d'expérience.

Faire l’examen

Informations générales sur l’examen

Les candidats sont tenus d'être présents au moins 30 minutes avant le début de l'examen. Les candidats qui arrivent en retard ne disposeront pas de temps supplémentaire pour compenser leur retard et pourraient se voir refuser l'accès à l'examen.

Les candidats doivent être en possession d'une carte d'identité valide (carte d'identité nationale, permis de conduire ou passeport) et la présenter au surveillant.

Si la demande en est faite le jour de l'examen, un délai supplémentaire peut être accordé aux candidats qui passent l'examen dans une langue autre que leur langue maternelle.

- 10 minutes supplémentaires pour les examens Foundation
- 20 minutes supplémentaires pour les examens Manager
- 30 minutes supplémentaires pour les examens Lead

Format et type d’examen PECB

1. **Examen au format papier** : Les examens sont imprimés, où les candidats ne sont pas autorisés à utiliser autre chose que le papier d'examen et un stylo. L'utilisation d'appareils électroniques, tels qu’ordinateurs portables, tablettes ou téléphones, n'est pas autorisée. La session d'examen est supervisée par un surveillant agréé par PECB sur le lieu où le partenaire a organisé la formation.
2. **Examen en ligne** : Les examens sont fournis par voie électronique via l'application PECB Exams. L'utilisation d'appareils électroniques, tels que les tablettes et les téléphones portables, n'est pas autorisée. La session d'examen est supervisée à distance par un surveillant de PECB via l'application PECB Exams et une caméra externe/intégrée.

Pour des informations plus détaillées sur le format d’examen en ligne, veuillez vous référer au PECB Online Exam Guide.

Les examens PECB sont disponibles en deux types :
1. Examen à développement
2. Examen à choix multiple

Cet examen contient des questions à choix multiple : Ce type d’examen a été choisi, car il s'est avéré efficace et efficient pour mesurer et évaluer les résultats d'apprentissage selon les domaines de compétence. L'examen à choix multiple peut être utilisé pour évaluer la compréhension d'un candidat sur de nombreux sujets, y compris des concepts simples ou complexes. Pour répondre à ces questions, les candidats devront appliquer divers principes, analyser des problèmes, évaluer des alternatives, combiner plusieurs concepts ou idées, etc.

Les questions à choix multiple sont basées sur un scénario, ce qui signifie qu'elles sont élaborées sur la base d'un scénario que les candidats sont invités à lire et qu'ils doivent fournir des réponses à une ou plusieurs questions liées à ce scénario. Cet examen à choix multiple est à livre ouvert, en raison de la caractéristique des questions qui dépendent du contexte. Vous trouverez ci-dessous un échantillon de questions d'examen.

L'examen étant « à livre ouvert », les candidats sont autorisés à utiliser les documents de référence suivants :

- Copie papier de la norme ISO/IEC 27001
- Support de formation du participant (accessible sur l'application PECB Exams ou imprimé)
- Notes personnelles prises pendant la session de formation (accessibles sur l'application PECB Exams ou papier)
- Dictionnaire au format papier

Toute tentative de copie, de collusion ou de tricherie pendant l'examen entraînera automatiquement un échec.

Les examens PECB sont disponibles en anglais et dans d'autres langues. Pour savoir si l'examen est disponible dans une langue particulière, veuillez contacter examination.team@pecb.com.

Note : PECB passera progressivement aux examens à choix multiples. Ils seront également à livre ouvert et comprendront des questions basées sur des scénarios qui permettront à PECB d'évaluer les connaissances, les capacités et les aptitudes des candidats à utiliser des informations dans de nouvelles situations (appliquer), à établir des liens entre des idées (analyser) et à justifier une position ou une décision (évaluer). Tous les examens à choix multiples de PECB comportent une question et trois alternatives, dont une seule est correcte.

Pour des informations spécifiques sur les types d'examens, les langues disponibles et d'autres détails, consultez la Liste des examens PECB.

Exemples de questions d'examen

Scénario :

La Compagnie A est une compagnie d'assurance dont le siège social est à Chicago. Elle offre une gamme variée de services et de produits, notamment des assurances médicales et automobiles. La société est récemment devenue l'une des plus grandes et des plus prospères compagnies d'assurance, avec plus de 70 bureaux à travers le monde.

Les objectifs de la compagnie sont de maintenir correctement ses actifs et de protéger la confidentialité des informations de ses clients. L'entreprise a décidé de se faire certifier ISO/IEC 27001, car cela l'aiderait non seulement à atteindre ses objectifs organisationnels et à se conformer aux lois et réglementations internationales, mais aussi à améliorer sa réputation. Elle a commencé à mettre en œuvre le SMSI en définissant une stratégie de mise en œuvre basée sur une analyse détaillée de ses processus existants et des exigences du SMSI. Elle a accordé une attention particulière à l'appréciation des risques liés à la sécurité de l'information, qui était essentielle pour comprendre les menaces et les vulnérabilités auxquelles elle était confrontée. Elle a également défini les critères de risque dans le but d'évaluer les risques identifiés.

La Compagnie A a connu une croissance rapide qui a entraîné un traitement complexe et intensif des données. Sur la base des résultats de l'appréciation des risques, elle a décidé de mettre à jour dans un premier temps son système de classification des informations existant, puis de mettre en œuvre les mesures de sécurité nécessaires en fonction du niveau de protection requis par chaque classification d'informations.

Les demandes de remboursement de frais médicaux de leurs clients, classées comme informations sensibles, ont été chiffrées à l'aide du chiffrement AES, puis déplacées vers le cloud privé. La Compagnie A a utilisé le stockage en cloud pour sa facilité d'accès. En raison de l'accès fréquent de ses employés à ce service, l'entreprise a également décidé d'utiliser le processus de journalisation. Le service a été configuré pour accorder automatiquement l'accès au stockage en cloud à tous les employés chargés de traiter les demandes de remboursement de frais médicaux.

Les services de stockage dans le cloud ayant connu des failles de sécurité dues à des erreurs humaines ou à des attaques délibérées, le service informatique de l'entreprise a décidé de restreindre l'accès aux informations sensibles stockées dans le cloud si les e-mails professionnels ne sont pas utilisés.
De plus, l'équipe a utilisé un logiciel de gestion des mots de passe pour gérer les mots de passe de ces adresses électroniques et générer des mots de passe plus forts.

Sur la base de ce scénario, répondez aux questions suivantes :

1. **Le service IT n'a pas restreint l'accès au stockage en cloud. Laquelle des menaces ci-dessous peut exploiter cette vulnérabilité ?**
   A. Piégeage de matériel
   B. **Utilisation non autorisée d'informations sensibles**
   C. Formation insuffisante sur le stockage en cloud

2. **La Compagnie A chiffre les informations sensibles avant de les déplacer vers le cloud. Quel principe de sécurité des informations est suivi dans ce cas ?**
   A. **Confidentialité, car le chiffrement garantit que seuls les utilisateurs autorisés peuvent accéder aux informations chiffrées.**
   B. Disponibilité, car le chiffrement garantit que les informations sont protégées au repos ou en transit, et donc accessibles en cas de besoin.
   C. Intégrité, car le chiffrement garantit que seules les modifications autorisées sont apportées aux informations chiffrées.

3. **La Compagnie A a décidé de restreindre l'accès aux informations sensibles stockées dans le cloud si les e-mails professionnels ne sont pas utilisés. Quelle mesure de sécurité a été mise en œuvre dans ce cas ?**
   A. Mesure de détection
   B. **Mesure préventive**
   C. Mesure corrective

4. **La Compagnie A a défini les critères de risque lors de l'appréciation de ses risques. Cela est-il nécessaire ?**
   A. **Oui, car l'entreprise doit établir et maintenir les critères de risque lors de l'appréciation des risques de sécurité de l'information.**
   B. Non, car les critères de risque ne doivent être établis que lorsque les options de traitement des risques sont définies.
   C. Non, car les critères de risque sont établis lorsque les risques résiduels de sécurité des informations sont acceptés.

Transmission des résultats d’examen

Les résultats d’examens seront communiqués par e-mail.

- Le délai de communication commence à la date de l'examen et dure de deux à quatre semaines pour les examens à choix multiple sur papier.
-
- Pour les examens à choix multiples en ligne, les candidats reçoivent leurs résultats instantanément.

Les candidats qui réussissent l'examen pourront se porter candidats à l'un des titres de compétences du programme de certification correspondant.

En cas d'échec à l'examen, une liste des domaines dans lesquels le candidat a obtenu une note inférieure à la note de passage sera ajoutée à l’e-mail pour aider les candidats à mieux se préparer à une reprise.

Politique de reprise d’examen

Il n’y a pas de limite au nombre de fois qu'un candidat peut reprendre un examen. Toutefois, il existe certains délais à respecter entre les reprises d'examen.

- Si le candidat échoue à l'examen à la 1re tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la tentative suivante (1re reprise).

Note : Les candidats qui ont suivi la formation auprès de l'un de nos partenaires et qui ont échoué à la première tentative d'examen peuvent se représenter gratuitement à l'examen dans un délai de 12 mois à compter de la date de réception du code promotionnel, car les frais payés pour la formation comprennent une première tentative d'examen et une reprise.)

Sinon, des frais de reprise s'appliquent.

ux candidats qui échouent à la reprise de l'examen, PECB recommande de suivre une formation afin d'être mieux préparé à l'examen.

Pour organiser une reprise d'examen, en fonction du format de l'examen, les candidats qui ont suivi une formation doivent suivre les étapes suivantes :

1. Examen en ligne : lors de l'organisation de la reprise de l'examen, utilisez le code coupon initial pour annuler les frais.
2. Examen sur papier : les candidats doivent contacter le partenaire/distributeur de PECB qui a organisé la session initiale pour organiser la reprise de l'examen (date, heure, lieu, coûts).

Les candidats qui n'ont pas suivi de formation avec un partenaire, mais qui se sont présentés à l'examen en ligne directement avec PECB, ne sont pas concernés par cette politique. La procédure pour organiser la reprise de l'examen est la même que pour l'examen initial.

Sécurité de l’examen

Une composante importante de la certification professionnelle est le maintien de la sécurité et de la confidentialité de l'examen. PECB compte sur le comportement éthique des titulaires et des candidats à la certification pour maintenir la sécurité et la confidentialité des examens PECB. Toute divulgation

d'informations sur le contenu des examens PECB constitue une violation directe du Code de déontologie de PECB. PECB prendra des mesures à l'encontre de toute personne qui enfreint les politiques et règlements, y compris l'interdiction permanente d'obtenir les certifications PECB et la révocation de toute certification antérieure. PECB intentera également une action en justice contre les personnes ou les organisations qui enfreignent ses droits d'auteur, ses droits de propriété et sa propriété intellectuelle.

Reprogrammer l'examen

Pour tout changement concernant la date, l'heure, le lieu de l'examen ou d'autres détails, veuillez contacter examination.team@pecb.com.

Demander la certification

Tous les candidats qui réussissent cet examen (ou un équivalent accepté par PECB) peuvent demander les titres de compétences de PECB pour lesquels ils ont été examinés. Des exigences spécifiques en matière d'éducation et d'expérience professionnelle doivent être remplies afin d'obtenir une certification PECB. Le candidat doit remplir le formulaire de demande de certification en ligne (accessible via son compte PECB), y compris les coordonnées des références qui seront contactées pour valider l'expérience professionnelle du candidat. Le candidat peut soumettre sa demande en plusieurs langues. Il peut choisir de payer en ligne ou d'être facturé. Pour de plus amples informations, veuillez contacter certification.team@pecb.com.

Le processus de demande de certification en ligne est très simple et ne prend que quelques minutes :

- Inscrivez-vous.
- Vérifier vos e-mails pour activer le lien de confirmation.
- Connectez-vous pour demander la certification

Pour plus d'informations sur le processus de demande, suivez les instructions du manuel Faire une demande de certification.

La demande est approuvée dès que le Service de certification valide que le candidat remplit toutes les exigences de certification relatives au titre concerné. Un e-mail sera envoyé à l'adresse électronique fournie au cours du processus de demande pour communiquer l'état de la demande.
Si la demande est approuvée, le candidat pourra télécharger la certification à partir de son compte PECB.

PECB offre un soutien en anglais et en français.

Renouveler la certification

Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Pour les conserver, les candidats doivent démontrer chaque année qu'ils effectuent toujours les activités liées à la certification. Les professionnels certifiés par PECB doivent fournir chaque année des unités de formation professionnelle continue (FPC) et payer 120 $ US de frais annuels de maintien (FAM) pour conserver leur certification. Pour de plus amples renseignements, veuillez consulter la page Maintien de la certification sur le site Web de PECB.

Fermeture d’un dossier

Si un candidat ne demande pas la certification dans les trois ans, son dossier sera fermé. Toutefois, même si la période de certification expire, le candidat a le droit de rouvrir son dossier. Cependant, PECB ne sera plus responsable de tout changement concernant les conditions, les normes, les politiques et le Manuel du candidat qui étaient applicables avant la fermeture du dossier. Un candidat qui demande la réouverture de son dossier doit le faire par écrit et payer les frais requis.

PECB

SECTION III : EXIGENCES DE CERTIFICATION

ISO/IEC 27001 Lead Implementer

Les exigences relatives à la certification « PECB ISO/IEC 27001 Implementer » sont les suivantes :

Titre de compétence	Examen	Expérience professionnelle	Expérience de projet SM	Autres exigences
PECB Certified ISO/IEC 27001 Provisional Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	Deux ans, dont un an d'expérience professionnelle en management de la sécurité de l'information	Activités de projet : total de 200 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Lead Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	Cinq ans dont deux ans d'expérience professionnelle en management de la sécurité de l'information	Activités de projet : total de 300 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Senior Lead Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	Dix ans dont sept ans d'expérience professionnelle en management de la sécurité de l'information	Activités de projet : total de 1 000 heures	Signer le Code de déontologie de PECB

Pour être considérées comme valides, les activités de mise en œuvre doivent suivre les bonnes pratiques de mise en œuvre et de management et inclure les éléments suivants :

1. Rédaction du plan SMSI
2. Initiation de la mise en œuvre du SMSI
3. Mise en œuvre du SMSI
4. Gestion, surveillance et maintien du SMSI
5. Identification et action sur les opportunités d'amélioration continue

SECTION IV : POLITIQUES ET RÈGLEMENTS RELATIFS À LA CERTIFICATION

Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. Les références professionnelles doivent provenir de personnes ayant travaillé avec le candidat dans un environnement professionnel et pouvant ainsi attester de son expérience de projet en sécurité de l'information, ainsi que de ses antécédents professionnels actuels et antérieurs. Les références professionnelles de personnes qui sont sous la supervision du candidat ou qui sont ses proches ne sont pas valables.

Expérience professionnelle

Le candidat doit fournir des informations complètes et exactes concernant son expérience professionnelle, notamment le titre de chaque poste, les dates de début et de fin, la description des postes, etc. Il est conseillé au candidat de résumer ses missions précédentes et actuelles, en fournissant suffisamment de détails pour décrire la nature des responsabilités de chaque emploi. Des informations plus détaillées peuvent être incluses dans le CV.

Expérience de projet SMSI

Le journal de projet SMSI du candidat sera vérifié pour s'assurer que le candidat a le nombre d'heures de projet requis.

Évaluation des demandes de certification

Le Service de certification évaluera chaque demande afin de valider l'éligibilité du candidat à la certification. Le candidat dont la demande est examinée en sera informé par écrit et disposera d'un délai raisonnable pour fournir tout document supplémentaire si nécessaire. Si un candidat ne répond pas dans le délai imparti ou ne fournit pas les documents requis dans le délai imparti, le service de certification validera la demande sur la base des informations initiales fournies, ce qui peut éventuellement conduire à la rétrogradation du candidat à un titre inférieur.

Refus de la demande de certification

PECB peut refuser la demande de certification si le candidat :

- Falsifie la demande
- Enfreint les procédures d'examen
- Enfreint le Code de déontologie de PECB
- Échoue à l'examen

Pour des informations plus détaillées, reportez-vous à la section **Plainte et appel**. Le paiement de la demande de certification n'est pas remboursable.

Suspension de la certification

PECB peut suspendre temporairement la certification si le candidat ne satisfait pas aux exigences de PECB. D'autres raisons peuvent justifier la suspension de la certification :

- PECB reçoit des plaintes excessives ou sérieuses de la part des parties intéressées (la suspension sera appliquée jusqu'à ce que l'enquête soit terminée).
- Les logos de PECB ou des organismes d'accréditation sont délibérément utilisés de manière abusive.
- Le candidat ne corrige pas l'usage abusif d'une marque de certification dans le délai déterminé par PECB.
- La personne certifiée a volontairement demandé une suspension.
- Toute autre condition jugée appropriée pour la suspension de la certification.

Révocation de la certification

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas aux exigences de PECB. Le candidat n'est alors plus autorisé à se présenter comme un professionnel certifié par PECB. D'autres raisons de révocation de la certification peuvent être invoquées si le candidat :

- Enfreint le Code de déontologie de PECB
- Fait une fausse déclaration et fournit de fausses informations sur la portée du certificat
- Enfreint toute autre règle de PECB

Mise à niveau des titres de compétences

Les professionnels peuvent demander à passer à une certification supérieure dès qu'ils peuvent démontrer qu'ils remplissent les conditions requises.

Pour faire une demande de mise à niveau, les candidats doivent se connecter à leur compte PECB, visiter l'onglet ***Mes certifications*** et cliquer sur le lien ***Mise à niveau***. Les frais de demande de mise à niveau sont de 100 $ US.

Déclassement des titres de compétences

Une certification PECB peut être déclassée à un titre inférieur pour les raisons suivantes :

- Les FAM n'ont pas été payés.
- Les heures de FPC n'ont pas été soumises.
- Un nombre insuffisant d'heures de FPC a été soumis.
- La preuve des heures de FPC n'a pas été soumise sur demande.

Note : *Les professionnels certifiés par PECB qui détiennent des certifications Lead et qui ne fournissent pas de preuves des exigences de maintien de la certification verront leurs titres déclassés. D'autre part, les détenteurs de certifications Master qui ne soumettent pas les FPC et ne paient pas les FAM verront leurs certifications révoquées.*

Autres statuts

En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour plus d'informations sur ces statuts et sur le statut de cessation permanente, ainsi que sur la manière de les appliquer, veuillez consulter la page État de la certification.

SECTION V: POLITIQUES GÉNÉRALES DE PECB

Code de déontologie de PECB

L'adhésion au Code de déontologie de PECB est un engagement volontaire. Il est important que les professionnels certifiés par PECB non seulement adhèrent aux principes de ce Code, mais aussi qu'ils encouragent et soutiennent les autres à faire de même. Plus d'informations sont disponibles ici.

Autres examens et certifications

PECB accepte les certifications et les examens d'autres organismes de certification accrédités et reconnus. PECB évaluera les demandes par le biais de son processus d'équivalence pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective (par exemple, la certification ISO/IEC 27001 Lead Auditor).

Non-discrimination et aménagements spéciaux

Toutes les candidatures seront évaluées objectivement, sans considération d'âge, de sexe, de race, de religion, de nationalité ou d'état civil du candidat.
Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB fera des aménagements raisonnables pour les candidats, le cas échéant. Si un candidat a besoin d'aménagements spéciaux en raison d'un handicap ou d'une condition physique particulière, il devrait en informer le partenaire/distributeur afin que celui-ci puisse prendre les dispositions nécessaires. Toute information fournie par les candidats concernant leur handicap/besoin sera traitée de manière strictement confidentielle.

Cliquez ici pour télécharger le Formulaire de demande d'aménagements spéciaux pour les candidats présentant un handicap.

Plainte et appel

Toute plainte doit être formulée au plus tard 30 jours après la réception de la décision de certification. PECB fournira une réponse écrite au candidat dans les 30 jours ouvrables suivant la réception de la plainte. Si la réponse de PECB n'est pas satisfaisante, le candidat a le droit de faire appel. Pour plus d'informations, consultez la Politique de plainte et d'appel de PECB ici.

(1) (1) Selon le Americans with Disabilities Act (ADA), le terme « aménagement raisonnable » peut inclure : (A) rendre les installations existantes utilisées par les employés facilement accessibles et utilisables par les individus souffrant d'invalidité ; et (B) la restructuration des tâches, les horaires de travail à temps partiel ou modifiés, la réaffectation à un poste vacant, l'acquisition ou la modification d'équipement ou d'appareils, l'adaptation ou la modification appropriée des examens, du matériel de formation ou des politiques, la fourniture de personnel qualifié.

(2) ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examens et cours. [Section 309] : Toute personne qui propose des examens ou des cours liés à des demandes, des licences, des certifications ou des habilitations pour l'enseignement secondaire ou post-secondaire, à des fins professionnelles ou commerciales, doit proposer ces examens ou ces cours dans un lieu et d'une manière accessibles aux personnes handicapées ou proposer d'autres arrangements accessibles à ces personnes.

PECB BEYOND RECOGNITION

Adresse :
Siège social 6683, rue
Jean-Talon Est,
Bureau 336 Montréal, QC,
CANADA H1S 0A5

Tel./Fax.
T : +1-844-426-7322
F : +1-844-329-7322

Centre d'aide de PECB
Visitez notre Centre d'aide pour parcourir la Foire aux questions (FAQ), consulter les manuels d'utilisation du site Web et des applications de PECB, lire les documents relatifs aux processus de PECB ou nous contacter via le système de suivi en ligne du centre d'aide.

E-mails
Examen : examination.team@pecb.com
Certification : certification.team@pecb.com
Service client : support@pecb.com