PECB

BEYOND RECOGNITION

ISO/IEC 27002 LEAD MANAGER

Manuel du candidat

PECB

Table des matières

PECB

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de formation qui offre des services de formation[1], de certification et des programmes de certificats aux personnes dans plusieurs disciplines.

Grâce à notre présence dans plus de 150 pays, nous aidons les experts et les organisations à faire preuve d'engagement et de compétence en leur fournissant une formation, une évaluation, une certification et des programmes de certification conformément à des normes rigoureuses et reconnues internationalement.

Nos principaux objectifs sont les suivants :

1. Établir les exigences minimales nécessaires à la certification des professionnels
2. Examiner et vérifier les qualifications des candidats pour qu'ils puissent être pris en considération pour l'évaluation de certification
3. Maintenir et améliorer continuellement le processus d'évaluation pour la certification des personnes
4. Certifier les personnes qualifiées, accorder les désignations et tenir à jour les répertoires respectifs
5. Établir des exigences pour le renouvellement périodique des certifications et s'assurer que les personnes certifiées se conforment à ces exigences
6. S'assurer que les professionnels de PECB respectent les normes éthiques dans leur pratique professionnelle
7. Représenter nos parties prenantes dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification et des programmes de certification auprès des professionnels, des entreprises, des gouvernements et du public

Notre mission

Notre mission est de fournir à nos clients des services d'examen, de certification et de programmes de certification complets qui inspirent confiance et enrichissent la société dans son ensemble.

Notre vision

Notre vision est de devenir la référence mondiale en matière de prestation de services de certification professionnelle et de programmes de certification..

Nos valeurs

Intégrité, professionnalisme, impartialité

[1]La formation fait référence aux formations développées par PECB et proposées dans le monde entier par l'intermédiaire de nos partenaires.

PECB

Valeur de la certification PECB

Reconnaissance mondiale
Les certifications PECB sont internationalement reconnues et accréditées par de nombreux organismes d'accréditation, de sorte que les professionnels qui les obtiennent bénéficient de notre reconnaissance sur les marchés nationaux et internationaux.

La valeur des certifications de PECB est validée par l'accréditation de l'International Accreditation Service (IAS-PCB-111), du United Kingdom Accreditation Service (UKAS-No. 21923) et du Korean Accreditation Board (KAB-PC-08) selon la norme ISO/IEC 17024 - Exigences générales relatives aux organismes procédant à la certification de personnes. La valeur des programmes de certification de PECB est validée par l'accréditation de l'ANSI National Accreditation Board (ANAB-Accreditation ID 1003) sous ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB est membre associé de l'Independent Association of Accredited Registrars (IAAR), membre à part entière de l'International Personnel Certification Association (IPC), membre signataire de l'IPC MLA, et membre du Club EBIOS, du CPD Certification Service, du CLUSIF, de Credential Engine et de l'ITCC. De plus, PECB est un Licensed Partner Publisher (LPP) agréé par le Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) pour la norme Cybersecurity Maturity Model Certification (CMMC), est agréé par le Club EBIOS pour proposer la certification EBIOS Risk Manager Skills, et est agréé par la CNIL (Commission nationale de l'informatique et des libertés) pour proposer la certification DPO. Pour davantage d'informations, cliquez ici.

Produits et services de haute qualité
Nous sommes fiers de fournir à nos clients des produits et des services de haute qualité qui répondent à leurs besoins et à leurs exigences. Tous nos produits sont soigneusement préparés par une équipe d'experts et de professionnels sur la base des meilleures pratiques et méthodologies.

Conformité aux normes
Nos certifications et nos programmes de certification démontrent la conformité aux normes ISO/IEC 17024 et ASTM E2659. Ils garantissent que les exigences de la norme ont été respectées et validées avec la cohérence, le professionnalisme et l'impartialité qui s'imposent.

Un service orienté vers le client
Nous sommes une entreprise orientée vers le client et nous traitons tous nos clients avec valeur, importance, professionnalisme et honnêteté. PECB dispose d'une équipe d'experts chargés de répondre aux demandes, aux questions et aux besoins. Nous faisons de notre mieux pour maintenir un délai de réponse maximal de 24 heures sans compromettre la qualité des services.

Flexibilité et commodité
Les possibilités d'apprentissage en ligne rendent votre parcours professionnel plus pratique, car vous pouvez programmer vos sessions d'apprentissage en fonction de votre mode de vie. Cette flexibilité vous donne plus de temps libre, vous offre plus de possibilités d'avancement professionnel et réduit les coûts.

PECB

Code de déontologie de PECB

Le Code de déontologie représente les valeurs et l'éthique les plus élevées que PECB s'engage à suivre, car il reconnaît leur importance lors de la prestation des services et de l'attraction des clients fidèles.

Le service de conformité veille à ce que les employés de PECB, les formateurs, les examinateurs, les surveillants, les partenaires, les distributeurs, les membres des différents conseils et comités consultatifs, les personnes certifiées et les titulaires de certificats (ci-après dénommés « professionnels de PECB ») respectent le présent code de déontologie. Le service de la conformité insiste également sur la nécessité d'adopter un comportement professionnel et de faire preuve de responsabilité, de compétence et d'équité dans la prestation de services aux parties prenantes internes et externes, telles que les candidats, les personnes certifiées, les détenteurs de certificats, les autorités d'accréditation et les autorités gouvernementales.

PECB est convaincu que pour réussir, l'organisation doit comprendre parfaitement les besoins et les attentes des clients et des parties prenantes. Pour y parvenir, PECB promeut une culture fondée sur les plus hauts niveaux d'intégrité, de professionnalisme et d'équité, qui sont également ses valeurs. Ces valeurs font partie intégrante de l'organisme et ont caractérisé la présence et la croissance mondiale au fil des ans et établi la réputation dont jouit PECB aujourd'hui.

PECB estime que des valeurs éthiques fortes sont essentielles pour entretenir des relations saines et solides. Par conséquent, il lui incombe en priorité de s'assurer que ses professionnels adoptent un comportement entièrement conforme aux principes et aux valeurs de PECB.

Les professionnels de PECB sont tenus de :

1. D'adopter un comportement professionnel lors de la prestation des services en faisant preuve d'honnêteté, de précision, d'équité et d'indépendance
2. Agir, en tout temps, pendant la prestation des services, uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, conformément au présent Code de déontologie et aux autres normes professionnelles
3. Démontrer et développer des compétences dans leurs domaines respectifs et s'efforcer d'améliorer continuellement leurs compétences et leurs connaissances
4. N'offrir que des services pour lesquels ils sont qualifiés et compétents et informer adéquatement les clients de la nature des services proposés, y compris de toute préoccupation ou de tout risque pertinent
5. Informer leur employeur ou leur client de tout intérêt commercial ou de toute affiliation qui pourrait influencer ou altérer leur jugement
6. Préserver la confidentialité des informations de tout employeur ou client actuel ou ancien pendant la prestation des services
7. Se conformer à toutes les lois et réglementations applicables dans les juridictions du pays où les prestations de services ont été effectuées
8. Respecter la propriété intellectuelle et les contributions d'autrui
9. Ne pas communiquer intentionnellement des informations fausses ou falsifiées susceptibles de compromettre l'intégrité du processus d'évaluation d'un candidat à une certification PECB ou à un programme de certification PECB
10. Ne pas se présenter faussement ou abusivement comme des représentants de PECB sans licence appropriée ni utiliser abusivement le logo, les certifications ou les certificats PECB

11. Ne pas agir d’une manière qui pourrait nuire à la réputation de PECB, aux certifications ou aux programmes de certification
12. Coopérer pleinement à l’enquête sur une prétendue violation du présent Code de déontologie

Pour lire la version complète du Code de déontologie de PECB consultez la page Code de déontologie de PECB.

Introduction à ISO/IEC 27002 Lead Manager

La norme ISO/IEC 27002 fournit des lignes directrices pour la mise en œuvre de mesures de sécurité de l'information afin de traiter les risques liés à la sécurité de l'information. La mise en œuvre de ces mesures de sécurité de l'information permettra aux organisations d'établir et d'appliquer efficacement des politiques et des mesures de contrôle pour garantir la sécurité de l'information conformément aux meilleures pratiques de l'industrie. La norme ISO/IEC 27002 peut être utilisée dans le cadre d'un système de management de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001.

La certification « ISO/IEC 27002 Lead Manager » démontre que vous possédez les compétences nécessaires pour mettre en œuvre, surveiller et améliorer continuellement les mesures de sécurité de l'information qui aident les organisations à protéger leurs informations. La formation offre une vue d'ensemble des principales approches et techniques de mise en œuvre des mesures de sécurité de l'information.

Les certifications PECB ne sont pas une licence ou une simple adhésion. Elles attestent des connaissances et des compétences acquises par les candidats dans le cadre de nos formations et sont délivrées aux candidats qui ont l'expérience requise et qui ont réussi l'examen.

Ce document spécifie le schéma de certification PECB ISO/IEC 27002 Lead Manager en conformité avec la norme ISO/IEC 17024:2012. Il décrit également les mesures que les candidats doivent prendre pour obtenir et conserver leurs titres. Il est donc très important de lire attentivement toutes les informations contenues dans ce document avant de remplir et d'envoyer votre demande. Si vous avez des questions ou si vous avez besoin d'informations complémentaires après l'avoir lu, veuillez contacter le bureau international de PECB à l'adresse suivantecertification.team@pecb.com.

PECB

SECTION II : PRÉPARATION DE L'EXAMEN, RÈGLES ET POLITIQUES

Préparation et programmation de l'examen

Les candidats sont responsables de leur propre étude et de leur préparation aux examens de certification. Bien que les candidats ne soient pas obligés de participer à la formation pour pouvoir se présenter à l'examen, le fait d'y assister peut augmenter de manière significative leurs chances de réussir l'examen.

Pour planifier l'examen, les candidats ont deux options :

1. Contactez l'un de nos partenaires agréés. Pour trouver un partenaire autorisé dans votre région, veuillez consulter la rubrique Partenaires actifs. Le calendrier des formations est également disponible en ligne et peut être consulté sur la page Événements de formationpagehttps://pecb.com/fr/partnerEvent/event_schedule_list
2. Passer un examen PECB à distance via l'application PECB Exams. Pour planifier un examen à distance, veuillez cliquer sur le lien suivant : Exam Events.

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.

Reprogrammer l'examen

Pour toute modification concernant la date, l'heure, le lieu de l'examen ou d'autres détails, veuillez contacter online.exams@pecb.com.

Frais de demande d'examen et de certification

Les candidats peuvent se présenter à l'examen sans participer à la formation. Les prix sont les suivants :

- Examen Lead : 1 000 $[2]
- Examen Manager : 700 $
- Examen Foundation : 500 $
- Examen Transition : 500 $

Les frais de demande de certification s'élèvent à $500.

Pour les candidats qui ont suivi la formation via l'un des partenaires de PECB, les frais d'inscription couvrent les coûts de l'examen (première tentative et première reprise), la demande de certification et la première année de frais de maintenance annuels (FAM).

[2] Tous les prix indiqués dans ce document sont en dollars américains.

PECB

Domaines de compétences

L'objectif de l'examen « PECB ISO/IEC 27002 Lead Manager » est de s'assurer que le candidat a acquis les connaissances et les compétences adéquates pour aider une organisation à sélectionner et à mettre en œuvre des mesures de sécurité de l'information appropriées pour traiter les risques liés à la sécurité de l'information.

La certification ISO/IEC 27002 Lead Manager est destinée aux :

- Responsables ou consultants souhaitant approfondir leurs connaissances en matière de mise en œuvre des mesures de sécurité de l'information
- Responsables ou consultants impliqués et concernés par la mise en œuvre d'un SMSI
- Personnes responsables du maintien de la conformité aux exigences de la norme ISO/IEC 27001 au sein d'une organisation
- Professionnels de TI ou consultants souhaitant approfondir leurs connaissances en matière de sécurité de l'information
- Membres d'une équipe de mise en œuvre du SMSI ou d'une équipe chargée de la sécurité de l'information

Le contenu de l'examen est divisé comme suit :

- **Domaine 1 :** Principes et concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée
- **Domaine 2 :** Système de management de la sécurité de l'information (SMSI) et lancement de la mise en œuvre des mesures de sécurité de la norme ISO/IEC 27002
- **Domaine 3 :** Mise en œuvre et gestion des mesures de sécurité relatives à l'organisation et au personnel, selon la norme ISO/IEC 27002
- **Domaine 4 :** Mise en œuvre et gestion des mesures de sécurité physique et technologique selon la norme ISO/IEC 27002
- **Domaine 5 :** Mesure des performances, tests et surveillance des mesures de sécurité de l'information selon la norme ISO/IEC 27002

PECB

Domaine 1 : Principes et concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée

Objectif principal : S'assurer que le candidat comprend et est capable d'interpréter les principaux concepts de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée.

Compétences	Énoncés de connaissances
1. Capacité à comprendre et à expliquer les principales normes de la famille ISO/IEC 27000 2. Capacité à comprendre et à expliquer les concepts de sécurité de l'information, de cybersécurité et de protection de la vie privée 3. Capacité à comprendre et à expliquer les trois grands principes de la sécurité de l'information (confidentialité, intégrité et disponibilité). 4. Capacité à comprendre et à expliquer la relation entre les vulnérabilités et les menaces 5. Capacité à comprendre et à expliquer l'objectif des différentes catégories de mesures de sécurité de l'information 6. Capacité à comprendre et à expliquer la définition du risque lié à la sécurité de l'information 7. Capacité à comprendre et à expliquer les composantes et les principes de la protection de la vie privée	1. Connaissance de la famille de normes ISO/IEC 27000 2. Connaissance des concepts de sécurité de l'information, de cybersécurité et de protection de la vie privée 3. Connaissance des trois grands principes de la sécurité de l'information (confidentialité, intégrité et disponibilité) 4. Connaissance de la relation entre les vulnérabilités et les menaces 5. Connaissance des catégories de mesures de sécurité de l'information et de leur finalité 6. Connaissance de la définition du risque de sécurité de l'information et de sa relation avec les autres composantes de la sécurité de l'information 7. Connaissance des principaux termes et définitions relatifs à la vie privée et aux principes de protection de la vie privée

PECB

Domaine 2 : Système de management de la sécurité de l'information (SMSI) et lancement de la mise en œuvre des mesures de sécurité de la norme ISO/IEC 27002

Objectif principal : S'assurer que le candidat comprend la définition d'un système de management de la sécurité de l'information (SMSI) et qu'il est capable de planifier la mise en œuvre des mesures de sécurité de la norme ISO/IEC 27002.

Compétences	Énoncés de connaissances
1. Capacité à comprendre et à expliquer la définition d'un système de management et les principales composantes d'un SMSI	1. Connaissance de la définition d'un système de management et des principales normes en la matière
2. Capacité à identifier et à utiliser les principales approches pour la mise en œuvre d'un SMSI	2. Connaissance du cycle « Planifier-Déployer-Contrôler-Agir » (PDCA)
3. Capacité à comprendre et à expliquer la structure de la norme ISO/IEC 27002	3. Connaissance des différences entre les normes ISO/IEC 27002:2013 et ISO/IEC 27002:2022
4. Capacité à distinguer et à expliquer les catégories de mesures de sécurité de l'information de la norme ISO/IEC 27002	4. Connaissance de la structure de la norme ISO/IEC 27002
5. Capacité à sélectionner et à utiliser les approches permettant d'analyser l'architecture de sécurité existante de l'organisation	5. Connaissance des mesures de sécurité organisationnelles, humaines, physiques et technologiques prévues par la norme ISO/IEC 27002
6. Capacité à effectuer une analyse des écarts et à rédiger un rapport d'analyse des écarts	6. Connaissance des principaux concepts et méthodes d'analyse d'une architecture de sécurité
7. Capacité à comprendre et à expliquer le processus de gestion des risques	7. Connaissance des techniques et des approches permettant de recueillir et d'interpréter les informations relatives à une architecture de sécurité
8. Capacité à sélectionner une méthode d'appréciation des risques appropriée	8. Connaissance des principaux concepts liés au risque
9. Effectuer les différentes étapes du processus d'appréciation des risques	9. Connaissance des critères à prendre en compte lors de la sélection d'une méthode d'appréciation des risques
10. Capacité à analyser et à déterminer le niveau de risque	10. Connaissance du processus d'appréciation des risques et de ses étapes
11. Capacité à identifier les options de traitement des risques et à élaborer un plan de traitement des risques	11. Connaissance des types d'analyse de risque, y compris l'analyse de risque qualitative, semi-quantitative et quantitative
12. Capacité à identifier et à sélectionner des mesures de sécurité adéquates afin de prévenir et d'atténuer les risques liés à la sécurité de l'information	12. Connaissance des options de traitement des risques (modification des risques, rétention des risques, évitement des risques et partage des risques)
13. Capacité à comprendre les éléments à prendre en compte lors de la préparation de la mise en œuvre des mesures de sécurité de l'information	

	13. Connaissance des principales approches pour la sélection des mesures de sécurité de l'information adéquates 14. Connaissance des mesures à prendre pour mettre en œuvre les mesures de sécurité de l'information sélectionnées

PECB

Domaine 3 : Mise en œuvre et gestion des mesures de sécurité relatives à l'organisation et au personnel, selon la norme ISO/IEC 27002

Objectif principal : S'assurer que le candidat comprend comment les mesures de sécurité organisationnelles et relatives aux personnes de la norme ISO/IEC 27002 doivent être mises en œuvre et gérées.

Compétences	Énoncés de connaissances
1. Capacité à comprendre et à expliquer les mesures de sécurité relatives à l'organisation et au personnel conformément à la norme ISO/IEC 27002 2. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant les politiques de sécurité de l'information 3. Capacité à attribuer et à gérer les rôles et les responsabilités en matière de sécurité de l'information sur la base des lignes directrices ISO/IEC 27002 4. Capacité à comprendre et à expliquer les exigences légales, statutaires, réglementaires et contractuelles ainsi que d'autres exigences en matière de sécurité de l'information 5. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour garantir la sécurité de l'information dans la gestion de projet et lors de l'utilisation de services en nuage 6. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour protéger les enregistrements et les procédures opérationnelles documentées 7. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour protéger la gestion de l'information et d'autres actifs associés 8. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant le contrôle d'accès, la gestion des identités et la gestion des droits d'accès 9. Capacité à comprendre et à mettre en œuvre les mesures de sécurité ISO/IEC 27002 relatives au processus d'embauche des employés, telles que la sélection, le	1. Connaissance des mesures de sécurité organisationnelles et relatives aux personnes prévues par la norme ISO/IEC 27002 2. Connaissance des processus relatifs à l'établissement des politiques de sécurité de l'information 3. Connaissance des lignes directrices ISO/IEC 27002 concernant les rôles et responsabilités en matière de gestion de la sécurité de l'information, la séparation des tâches et les responsabilités de la direction 4. Connaissance des exigences légales, statutaires, réglementaires et contractuelles et respect des politiques, règles et normes en matière de sécurité de l'information 5. Connaissance des pratiques de sécurité de l'information pour la gestion de projet et les services en nuage 6. Connaissance des mesures de sécurité de l'information nécessaires pour assurer la protection des enregistrements et des données à caractère personnel (DCP) 7. Connaissance du concept de renseignements sur les menaces et de ses différents types 8. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 relatives à la gestion des actifs et à la classification et au marquage des informations 9. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 relatives au contrôle d'accès, à la gestion des identités et à la gestion des droits d'accès 10. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 concernant le processus de recrutement des employés 11. Connaissance des lignes directrices ISO/IEC 27002 concernant les programmes de

licenciement ou le changement d'emploi, ainsi que les conditions d'emploi
10. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant la sensibilisation à la sécurité de l'information et les programmes de formation
11. Capacité à communiquer, à surveiller et à gérer les rôles et les responsabilités en matière de sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27002
12. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 afin de garantir la sécurité des informations concernant les relations avec les fournisseurs
13. Capacité à réviser et à surveiller les services des fournisseurs en termes de sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27002
14. Capacité à comprendre et à expliquer le concept d'analyse de l'impact sur les activités et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant les plans de continuité d'activité
15. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant les incidents liés à la sécurité de l'information

sensibilisation et de formation à la sécurité de l'information
12. Connaissance des lignes directrices de la norme ISO/IEC 27002 applicables aux employés pour assurer la protection des informations confidentielles
13. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 concernant les relations avec les fournisseurs et la gestion de la sécurité de l'information dans la chaîne d'approvisionnement des TIC
14. Connaissance des lignes directrices de la norme ISO/IEC 27002 visant à garantir la sécurité de l'information en ce qui concerne les accords avec les fournisseurs
15. Connaissance des lignes directrices de la norme ISO/IEC 27002 visant à assurer la protection des systèmes TIC en cas d'interruption
16. Connaissance des lignes directrices de la norme ISO/IEC 27002 pour la gestion des incidents de sécurité de l'information, y compris la planification et la préparation, l'évaluation et la décision, la réponse et l'apprentissage à partir des incidents de sécurité de l'information

PECB

Domaine 4 : Mise en œuvre et gestion des mesures de sécurité physique et technologique selon la norme ISO/IEC 27002

Objectif principal : S'assurer que le candidat est en mesure d'identifier et de comprendre les lignes directrices de la norme ISO/IEC 27002 concernant la gestion des mesures de sécurité physiques et technologiques.

Compétences	Énoncés de connaissances
1. Capacité à comprendre l'objectif des mesures de sécurité physique et technologique de la norme ISO/IEC 27002	1. Connaissance des mesures de sécurité physiques et technologiques de la norme ISO/IEC 27002
2. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant les périmètres de sécurité physique	2. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant le périmètre de sécurité physique et les contrôles d'entrée physiques
3. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant la sécurité des bureaux, des salles et des autres installations	3. Connaissance des lignes directrices de la norme ISO/IEC 27002 relatives à la sécurité des bureaux, des salles et des installations.
4. Capacité à utiliser et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 et d'autres bonnes pratiques pour protéger les locaux d'une organisation contre les menaces physiques et environnementales	4. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 concernant les zones sécurisées
5. Capacité à comprendre et à mettre en œuvre la politique du bureau vide et de l'écran vide selon les lignes directrices de la norme ISO/IEC 27002	5. Connaissance de la politique de bureau vide et d'écran vide de la norme ISO/IEC 27002
6. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour sécuriser les supports de stockage et les matériels	6. Connaissance des lignes directrices de la norme ISO/IEC 27002 relatives à la gestion des supports de stockage et à la protection des matériels
7. Capacité à établir un plan de maintenance des matériels sur la base des lignes directrices de la norme ISO/IEC 27002	7. Connaissance des lignes directrices ISO/IEC 27002 concernant le plan de maintenance des matériels
8. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour assurer la protection contre les logiciels malveillants	8. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant la protection des informations contre les codes malveillants
9. Capacité à gérer les vulnérabilités techniques sur la base des lignes directrices de la norme ISO/IEC 27002	9. Connaissance du dimensionnement et de la gestion des configurations sur la base des lignes directrices de la norme ISO/IEC 27002
10. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC	10. Connaissance du processus de masquage des données et des mesures de prévention des fuites de données conformément à la norme ISO/IEC 27002
	11. Connaissance du concept de cryptographie et de sa gestion sur la base des lignes directrices de la norme ISO/IEC 27002
	12. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 relatives au cycle de

27002 concernant l'anonymisation et la pseudonymisation des données
11. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 concernant la cryptographie asymétrique et symétrique
12. Capacité à comprendre et à mettre en œuvre les mesures de sécurité de la norme ISO/IEC 27002 afin de garantir la sécurité des applications tout au long de leur cycle de développement
13. Capacité à comprendre et à mettre en œuvre les mesures de sécurité de la norme ISO/IEC 27002 concernant les terminaux finaux, les enregistrements et la synchronisation des horloges
14. Capacité à comprendre et à mettre en œuvre les mesures de sécurité de la norme ISO/IEC 27002 qui garantissent un accès autorisé à l'information et aux autres actifs associés
15. Capacité à comprendre et à mettre en œuvre les mesures de sécurité de la norme ISO/IEC 27002 relatives à la protection des réseaux

développement sécurisé, à l'architecture du système et au codage
13. Connaissance des mesures de sécurité de la norme ISO/IEC 27002 relatives à la gestion des droits d'accès privilégiés et à l'utilisation de programmes utilitaires privilégiés
14. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant la gestion des identités et des accès privilégiés
15. Connaissance des lignes directrices de la norme ISO/IEC 27002 qui traitent des risques liés à l'accès non autorisé au code source
16. Connaissance des processus d'enregistrement et de révision des journaux sur la base des lignes directrices de la norme ISO/IEC 27002
17. Connaissance des lignes directrices de la norme ISO/IEC 27002 visant à garantir la sécurité des réseaux

PECB

Domaine 5 : Mesure des performances, tests et surveillance des mesures de sécurité de l'information selon la norme ISO/IEC 27002

Objectif principal : S'assurer que le candidat est en mesure de comprendre les mesures de sécurité de l'information selon la norme ISO/IEC 27002 et de mener des activités de mesure et de surveillance des performances sur la base de la norme ISO/IEC 27002

Compétences	Énoncés de connaissances
1. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour tester la sécurité de l'information	1. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant les étapes du cycle de vie des tests de logiciels et des meilleures techniques et outils de test de sécurité
2. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour garantir la sécurité de l'information des services externalisés	2. Connaissance des activités de surveillance et de révision liées au développement de systèmes externalisés sur la base des lignes directrices de la norme ISO/IEC 27002
3. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour la protection de l'environnement opérationnel	3. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant les environnements de développement de logiciels, y compris le développement, la simulation et l'opérationnel
4. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 pour la protection des informations de test	4. Connaissance des lignes directrices de la norme ISO/IEC 27002 qui traitent des risques d'accès ou d'utilisation non autorisés des informations relatives aux tests
5. Capacité à comprendre et à mettre en œuvre les lignes directrices de la norme ISO/IEC 27002 relatives à la protection des systèmes d'information pendant les tests d'audit	5. Connaissance des lignes directrices de la norme ISO/IEC 27002 relatives à la protection des systèmes d'information pendant les tests d'audit
6. Capacité à réaliser des révisions indépendantes de la sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27002	6. Connaissance des lignes directrices de la norme ISO/IEC 27002 relatives à la révision de la sécurité de l'information
7. Capacité à comprendre et à mettre en œuvre les meilleures pratiques en matière de surveillance du réseau	7. Connaissance des techniques de surveillance des réseaux
8. Capacité à comprendre et à mettre en œuvre des processus d'amélioration continue basés sur les lignes directrices de la norme ISO/IEC 27002	8. Connaissance des meilleures approches utilisées pour surveiller l'efficacité des mesures de la sécurité de l'information
9. Capacité à sélectionner et à mettre en œuvre les approches appropriées pour maintenir la sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27002	9. Connaissance des lignes directrices de la norme ISO/IEC 27002 concernant les activités d'amélioration continue

Selon les domaines susmentionnés et leur pertinence, l'examen contient 80 questions à choix multiples, comme le résume 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 l'évaluation
Domaines de compétences	Principes et concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée	10	12.5	X	
	Système de management de la sécurité de l'information (SMSI) et lancement de la mise en œuvre des mesures de sécurité de la norme ISO/IEC 27002	10	12.5	X	
	Mise en œuvre et gestion des mesures de sécurité relatives à l'organisation et au personnel, selon la norme ISO/IEC 27002	20	25		X
	Mise en œuvre et gestion des mesures de sécurité physique et technologique selon la norme ISO/IEC 27002	20	25		X
	Mesure des performances, tests et surveillance des mesures de sécurité de l'information selon la norme ISO/IEC 27002	20	25	X	
	Total des points	**80**	**100 %**		
	Nombre de questions par niveau de compréhension			**40**	**40**
	Pourcentage de l'examen consacré à chaque niveau de compréhension (cognitif/taxonomie)			**50%**	**50%**

La note de passage est établie à **70 %**.
Après avoir réussi l'examen, les candidats pourront demander à obtenir le certificat « PECB Certified ISO/IEC 27002 Lead Manager ».

PECB

Passer 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 plus d’informations sur les examens en ligne, consultez le Guide de l’examen en ligne .

Les examens PECB sont disponibles en deux types :

1. Examen à développement
2. Examen à choix multiple

Cet examen est composé de questions à choix multiples : L’examen à choix multiples peut être utilisé pour évaluer la compréhension des candidats sur des concepts simples ou complexes. Il comprend à la fois des questions autonomes et des questions basées sur des scénarios. Les questions autonomes sont indépendantes de l’examen et ne dépendent pas du contexte, alors que les questions basées sur un scénario dépendent du contexte, c’est-à-dire qu’elles sont élaborées sur la base d’un scénario que le candidat doit lire et pour lequel il doit répondre à cinq questions liées à ce scénario. En répondant aux questions autonomes et aux questions basées sur des scénarios, les candidats devront appliquer divers concepts et principes expliqués au cours de la formation, analyser des problèmes, identifier et évaluer des alternatives, combiner plusieurs concepts ou idées, etc.

Chaque question à choix multiple comporte trois options, dont l’une est la bonne réponse (la réponse clé) et les deux autres sont des réponses incorrectes (les distracteurs).

Il s’agit d’un examen à livre ouvert. Le candidat est autorisé à utiliser les documents de référence suivants :

- Une copie papier de la norme ISO/IEC 27002
- Matériel de formation (accessible via l’application PECB Exams et/ou imprimé)
- Toutes les notes personnelles prises pendant la formation (accessibles via l’application PECB Exams et/ou imprimées).
- Dictionnaire au format papier

Un exemple de questions d’examen est fourni ci-après.

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).

Pour obtenir des informations spécifiques sur les types d’examens, les langues disponibles et d’autres détails, veuillez contacter examination.team@pecb.com ou consulter la liste des examens de PECB.

Exemples de questions d'examen

ChereX est un fabricant américain de produits électroniques. L'entreprise vise à fournir des produits électroniques avancés qui répondent aux besoins des clients. Avec l'évolution des technologies, l'industrie de la fabrication électronique est devenue la cible de cyberattaques. C'est pourquoi *ChereX*a investi de manière significative dans la création de systèmes sécurisés et d'une culture de la sécurité durable. Dans le cadre de ces initiatives, *ChereX* a décidé de mettre en place un système de management de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001. Elle a également utilisé les lignes directrices de la norme ISO/IEC 27002 dans le cadre de la mise en œuvre du système de management de la sécurité des informations.

Sur la base des lignes directrices de la norme ISO/IEC 27002, *ChereX* a mis en place un programme de sensibilisation et de formation à la sécurité de l'information qui a permis à la direction générale de s'assurer que tous les employés comprennent leur rôle et leurs responsabilités en matière de sécurité de l'information. Les sessions de sensibilisation et de formation à la sécurité de l'information ont lieu chaque trimestre et sont adaptées aux rôles et fonctions des différents départements. Le programme de sensibilisation et de formation à la sécurité de l'information de *ChereX* comprend diverses discussions concernant les politiques de sécurité de l'information et les responsabilités de chaque employé pour protéger les actifs de l'organisation.

ChereX a également mené un processus d'appréciation des risques afin d'identifier et d'analyser les risques liés à ses systèmes d'information. En suivant la méthodologie d'appréciation des risques du ChereX, le responsable de la sécurité de l'information a identifié les actifs, les menaces, les vulnérabilités et les sources de risque. La liste des actifs inclut des supports de stockage endommagés contenant des données sensibles. En l'absence de procédure de gestion des supports de stockage au sein de l'entreprise, ces terminaux ont été placés dans les bureaux de *ChereX* sans mesures appropriées pour les protéger contre les accès non autorisés. Le risque d'accès non autorisé à des informations sensibles par l'intermédiaire de ces terminaux étant défini comme « élevé », *ChereX* a décidé de les détruire immédiatement. Le responsable de la sécurité de l'information a élaboré une politique spécifique sur la gestion des supports de stockage. Le responsable de la sécurité de l'information a ensuite approuvé la politique et l'a communiquée au département informatique.

Sur la base du scénario ci-dessus, répondez aux questions suivantes :

1. ***ChereX* a utilisé la norme ISO/IEC 27002 comme norme d'appui pour la mise en œuvre du SMSI conformément à la norme ISO/IEC 27001. Est-ce acceptable ?**
   A. **Oui, les lignes directrices de la norme ISO/IEC 27002 peuvent être utilisées dans le cadre d'un SMSI**
   B. Non, seules les lignes directrices de la norme ISO/IEC 27002 doivent être utilisées pour mettre en œuvre un SMSI
   C. Non, la norme ISO/IEC 27002 ne peut être utilisée que par les organisations qui ont déjà mis en place un SMSI

2. ***ChereX* a immédiatement mis en œuvre des mesures de sécurité pour traiter le risque concernant les terminaux qui contiennent des données sensibles. Une telle décision est-elle conforme aux lignes directrices de la norme ISO/IEC 27002 ?**
   A. Oui, *ChereX* doit détruire physiquement tous les terminaux endommagés qui contiennent des données sensibles
   B. **Non, *ChereX* doit procéder** à une **appréciation des risques liés aux terminaux endommagés afin de déterminer s'ils doivent être détruits physiquement**
   C. Non, *ChereX* doit réparer les terminaux endommagés et veiller à ce que les informations sensibles ne soient pas supprimées avant leur élimination ou leur réutilisation

3. ***ChereX* a mis en place un programme de sensibilisation à la sécurité de l'information. Selon les lignes directrices de la norme ISO/IEC 27002, quel type de mesure de sécurité a été mise en place par *ChereX* ?**
   A. Organisationnelle
   B. **Relative aux personnes**
   C. Technologique

4. ***ChereX* a-t-elle suivi toutes les lignes directrices de la norme ISO/IEC 27002 lors de l'élaboration de la politique spécifique concernant la gestion des supports de stockage ?**
   A. **Non, les politiques spécifiques à un thème doivent être approuvées par la direction générale**
   B. Non, les politiques spécifiques à un thème doivent être communiquées et reconnues par l'ensemble du personnel de l'entreprise
   C. Oui, la politique spécifique a été élaborée et approuvée par le responsable de la sécurité de l'information et communiquée au personnel concerné

PECB

Politique de sécurité des examens

PECB s'engage à protéger l'intégrité de ses examens et de l'ensemble du processus d'examen, et compte sur le comportement éthique des candidats, des candidats potentiels, des candidats et des partenaires pour maintenir la confidentialité des examens de PECB. Cette politique vise à lutter contre les comportements inacceptables et à garantir un traitement équitable de tous les candidats.

Toute divulgation d'informations sur le contenu des examens de PECB constitue une violation directe de la présente politique et du code déontologique de PECB. Par conséquent, les candidats qui se présentent à un examen du PECB sont tenus de signer un accord de confidentialité et de non-divulgation de l'examen et doivent se conformer à ce qui suit :

1. Les questions et réponses du matériel d'examen sont la propriété exclusive et confidentielle de PECB. Une fois que les candidats ont soumis l'examen à PECB, ils n'ont plus accès à l'examen original ou à une copie de celui-ci.
2. Il est interdit aux candidats de révéler toute information concernant les questions et les réponses de l'examen ou de discuter de ces détails avec un autre candidat ou une autre personne.
3. Les candidats ne sont pas autorisés à emporter en dehors de la salle d'examen tout matériel lié à l'examen.
4. Les candidats ne sont pas autorisés à copier ou à tenter de faire des copies (écrites, photocopiées ou autres) du matériel d'examen, y compris, mais sans s'y limiter, des questions, des réponses ou des copies d'écran.
5. Les candidats ne doivent pas participer à des activités frauduleuses liées à la passation d'examens ni en faire la promotion, comme par exemple :
    - Regarder le matériel d'examen ou la feuille de réponse d'un autre candidat
    - Donner ou recevoir de l'aide d'un surveillant, d'un candidat ou de toute autre personne
    - Utiliser des guides de référence, des manuels, des outils, etc. non autorisés, y compris des sites de « brain dumping », car ils ne sont pas autorisés par PECB.

Dès qu'un candidat a connaissance ou est déjà au courant d'irrégularités ou de violations des points mentionnés ci-dessus, il est responsable de s'y conformer, sinon, si de telles irrégularités se produisent, les candidats seront directement dénoncés auprès de PECB ou, s'ils sont témoins de telles irrégularités, ils doivent immédiatement les signaler à PECB.

Les candidats sont seuls responsables de la compréhension et du respect des règles et politiques d'examen de PECB, de l'accord de confidentialité et de non-divulgation et du code de déontologie. Par conséquent, si une violation d'une ou de plusieurs règles est constatée, les candidats ne recevront aucun remboursement. Par ailleurs, PECB a le droit de refuser le droit de se présenter à un examen PECB ou d'inviter les candidats à repasser l'examen si des irrégularités sont identifiées pendant et après le processus de notation, en fonction de la gravité du cas.

Toute violation des points mentionnés ci-dessus causera à PECB des dommages irréparables qu'aucune réparation pécuniaire ne pourra compenser. Par conséquent, PECB peut prendre les mesures appropriées pour remédier ou empêcher toute divulgation non autorisée ou utilisation abusive du matériel d'examen, y compris l'obtention d'une injonction immédiate.

PECB prendra des mesures à l'encontre des personnes qui enfreignent les règles et les politiques, y compris l'interdiction permanente d'obtenir des certificats de PECB et la révocation de tout certificat antérieur. 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.

Résultats de l'examen

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

- Le délai de communication commence à la date de l'examen et dure de trois à huit semaines pour les examens de type rédactionnel et de deux à quatre semaines pour les examens à choix multiples 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.

Les candidats qui ne sont pas d'accord avec les résultats peuvent demander une réévaluation en adressant un courrier à examination.team@pecb.comdans les 30 jours suivant la réception des résultats. Les demandes de réévaluation reçues après 30 jours ne seront pas traitées. Si les candidats ne sont pas d'accord avec les résultats de la réévaluation, ils disposent de 30 jours à compter de la date à laquelle ils ont reçu les résultats de l'examen réévalué pour déposer une plainte via PECB Ticketing System. Toute plainte reçue après 30 jours ne sera pas traitée.

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 un candidat ne réussit pas l'examen lors de la première tentative, il doit attendre 15 jours après la date initiale de l'examen pour la tentative suivante (1re reprise).

Note : Les candidats qui ont suivi la formation chez l'un de nos partenaires et qui ont échoué à la première tentative d'examen peuvent repasser gratuitement l'examen dans un délai de 12 mois à compter de la date de réception du code coupon (les frais payés pour la formation comprennent une première tentative d'examen et une deuxième tentative). 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 formations 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.

PECB

SECTION III : PROCESSUS ET EXIGENCES DE CERTIFICATION

Certificats ISO/IEC 27002 de PECB

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

Les certifications du programme ISO/IEC 27002 de PECB répondent aux exigences suivantes :

Titre de compétence	Enseignement	Examen	Expérience professionnelle	Expérience en management de la sécurité de l'information	Autres exigences
PECB Certified ISO/IEC 27002 Provisional Manager	Au moins l'enseignement secondaire	Examen PECB Certified ISO/IEC 27002 Lead Manager ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27002 Manager			Deux ans : Une année d'expérience professionnelle dans la gestion de la sécurité de l'information	Activités de projet : total de 200 heures	
PECB Certified ISO/IEC 27002 Lead Manager			Cinq ans : Deux ans d'expérience professionnelle dans la gestion de la sécurité de l'information	Activités de projet : total de 300 heures	
PECB Certified ISO/IEC 27002 Senior Lead Manager			Dix ans : Sept ans d'expérience professionnelle dans la gestion de la sécurité de l'information	Activités de projet : total de 1 000 heures	

Pour être considérées comme valides, les activités doivent respecter les bonnes pratiques en matière de sécurité de l'information et inclure les éléments suivants :

1. Rédaction d'un plan de mise en œuvre du SMSI
2. Gestion d'un projet de mise en œuvre de la sécurité de l'information
3. Mise en œuvre des processus de sécurité de l'information
4. Sélection des mesures de sécurité de l'information
5. Mise en œuvre et évaluation des mesures de sécurité de l'information

Demande de certification

Tous les candidats qui ont réussi l'examen (ou un équivalent accepté par PECB) sont autorisés à demander la certification PECB pour laquelle ils ont été évalués. Des exigences spécifiques en matière d'éducation et d'expérience professionnelle doivent être remplies afin d'obtenir une certification PECB. Les candidats

doivent remplir le formulaire de demande de certification en ligne (accessible via leur compte PECB), y compris les coordonnées des personnes qui seront contactées pour valider l'expérience professionnelle des candidats. Les candidats peuvent soumettre leur candidature en anglais, français, allemand, espagnol ou coréen. Ils peuvent choisir de payer en ligne ou d'être facturés. Pour plus d'informations, veuillez contacter certification.team@pecb.com.

La procédure de demande de certification en ligne est très simple et ne prend que quelques minutes :

- Créer votre compte
- Vérifier vos e-mails pour activer le lien de confirmation.
- Se connecter pour demander la certification

Pour plus d'informations sur la procédure de demande de certification, cliquez ici.

Le service de certification valide que le candidat remplit toutes les conditions de certification pour le titre concerné. Le service de certification valide que le candidat remplit toutes les conditions de certification pour le titre concerné.

Une fois la demande approuvée par le service de certification, le candidat pourra télécharger le certificat et réclamer le badge numérique correspondant. Pour plus d'informations sur le téléchargement du certificat, cliquez ici , et pour plus d'informations sur l'obtention du badge numérique, cliquez ici.

PECB fournit une assistance en anglais et en français.

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.

Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. Elles doivent émaner de personnes qui ont travaillé avec le candidat dans un environnement professionnel et qui peuvent valider son expérience en matière de gestion de la sécurité de l'information, ainsi que 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 des projets de gestion de la sécurité de l'information

Le journal de projet du candidat sera vérifié pour s'assurer que le candidat a le nombre requis d'heures de gestion de la sécurité de l'information.

Évaluation des demandes de certification

Le service de certification évaluera chaque demande afin de valider l'éligibilité des candidats à la certification ou au programme de 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 à la date limite ou ne fournit pas la documentation requise dans le délai imparti, le service de certification validera la demande sur la base des informations initiales fournies, ce qui peut entraîner une dégradation des compétences du candidat.

PECB

SECTION IV : POLITIQUES DE CERTIFICATION

Refus de certification

PECB peut refuser la certification/le programme de certification si le candidat :

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

Les candidats dont le programme de certification/certificat a été refusé peuvent déposer une plainte dans le cadre de la procédure de plainte et de recours. Pour de plus amples informations, veuillez vous référer à la section **Procédure de plainte et de recours.**

Le paiement de la demande pour le programme de certification/certificat n'est pas remboursable.

Options de statut de certification

Active

Cela signifie que votre certification est en règle et valide, et qu'elle est maintenue en remplissant les exigences du PECB concernant le CPD et les FAM.

Suspendue

PECB peut suspendre temporairement la certification des candidats s'ils ne satisfont pas aux exigences. D'autres raisons peuvent justifier la suspension de la certification :

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

Révocation

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas à ses exigences. Le candidat n'est alors plus autorisé à se présenter comme un professionnel certifié par PECB. La révocation s'applique également si le candidat :

- Enfreint le Code de déontologie de PECB
- Déforme ou fournit de fausses informations sur la portée de la certification/programme de certification
- Enfreint toute autre règle de PECB
- Toute autre raison que PECB juge appropriée

Les candidats dont la certification a été révoquée peuvent déposer une plainte dans le cadre de la procédure de réclamation et de recours. Pour de plus amples informations, veuillez vous référer à la section **Procédure de plainte et de recours.**

Autres statuts
En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour en savoir plus sur ces statuts et sur le statut de cessation permanente, voir Certification Status Options.

Mise à niveau et rétrogradation des certificats

Mise à niveau des certificats
Les professionnels peuvent mettre à niveau leurs certificats dès qu'ils peuvent démontrer qu'ils remplissent les conditions requises.

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

Rétrogradation des certificats
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 la preuve qu'ils respectent les exigences de maintien de la certification verront leurs titres rétrogradés. Les titulaires d'une certification Master qui ne soumettent pas de CPD et ne paient pas les FMA verront leur certification révoquée.*

Renouvellement de la certification
Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Pour les conserver, les professionnels certifiés par PECB doivent satisfaire aux exigences liées au titre désigné, par exemple, ils doivent effectuer le nombre requis d'heures de développement professionnel continu (DPC). En outre, ils doivent s'acquitter des frais annuels de maintenance (120 $). Pour plus d'informations, consultez la page Certification Maintenance sur le site web de PECB.

Clôture d'un dossier
Si les candidats ne présentent pas de demande de certification dans un délai d'un an, leur dossier sera clôturé. 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. Le candidat qui demande la réouverture de son dossier doit le faire par écrit à l'adresse certification.team@pecb.com et s'acquitter de la taxe requise.

Politique en matière de plaintes et de recours

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 les candidats ne sont pas satisfaits de la réponse, ils ont le droit d'introduire un recours.

Pour plus d'informations sur la politique en matière de plaintes et de recours, cliquez ici.

PECB

SECTION V : POLITIQUES GÉNÉRALES

Examens et certifications d'autres organismes de certification accrédités

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 afin de 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 27002 Lead Manager).

Non-discrimination et aménagements spéciaux

Toutes les candidatures seront évaluées objectivement, indépendamment de l'âge, du sexe, de la race, de la religion, de la nationalité ou de l'état civil des candidats.

Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB mettra en place des aménagements[3] raisonnables pour les candidats, le cas échéant. Si les candidats ont besoin d'aménagements particuliers en raison d'un handicap ou d'une condition physique spécifique, ils doivent en informer le partenaire/distributeur afin qu'il prenne les dispositions[4] nécessaires. Toute information fournie par les candidats concernant leur handicap ou leurs besoins particuliers sera traitée de manière confidentielle. Pour télécharger le formulaire, cliquez ici.

Politique en matière de comportement

PECB aspire à fournir des services de qualité supérieure, cohérents et accessibles à ses parties prenantes externes : distributeurs, partenaires, formateurs, surveillants, examinateurs, membres des différents comités et conseils consultatifs, et clients (stagiaires, candidats à l'examen, personnes certifiées et titulaires de certificats), ainsi qu'à créer et maintenir un environnement de travail positif qui assure la sécurité et le bien-être de son personnel, et qui tient en haute estime la dignité, le respect et les droits de l'homme de son personnel.

L'objectif de cette politique est de s'assurer que PECB gère de manière impartiale, confidentielle, équitable et opportune les comportements inacceptables des parties prenantes externes à l'égard du personnel de PECB. Pour lire la politique en matière de comportement, cliquez ici.

Politique de remboursement

PECB vous remboursera votre paiement si les conditions de la politique de remboursement sont remplies. Pour lire la politique de remboursement, cliquez ici.

---

[3] Selon l'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.

[4] 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.

Adresse :

Siège social
6683, rue Jean-Talon Est,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax :

T : +1-844-426-7322
F : +1-844-329-7322

Emails :

Examen :
examination.team@pecb.com

Certification :
certification.team@pecb.com

Service clientèle :
support@pecb.com

Centre d'aide de PECB

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

www.pecb.com