PECB

BEYOND RECOGNITION

Lead Cybersecurity Manager

Manuel du candidat

Table des matières

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui propose des services de formation[1] et de certification de personnes dans un large éventail de disciplines.

Grâce à notre présence dans plus de 150 pays, nous aidons les professionnels à démontrer leurs compétences dans divers domaines d'expertise en leur proposant des programmes d'évaluation et de certification conformes à des normes internationalement reconnues.

Nos principaux objectifs sont les suivants :

1. Établir les exigences minimales nécessaires pour certifier les professionnels et octroyer les certifications
2. Examiner et vérifier les qualifications des personnes pour s'assurer qu'elles sont éligibles à la certification
3. Maintenir et améliorer continuellement le processus d'évaluation pour la certification des personnes
4. Certifier les personnes qualifiées, octroyer les certifications et tenir à jour les répertoires correspondants.
5. Établir les exigences pour le renouvellement périodique de la certification et veiller au respect de ces exigences par les personnes certifiées
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

Fournir à nos clients des services complets d'examen et de certification qui inspirent la confiance et profitent à l'ensemble de la société.

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]Le terme « formation » fait référence aux formations élaborées par PECB et proposées dans le monde entier via les partenaires de PECB.

Valeur de la certification PECB

Reconnaissance mondiale
Les certifications PECB sont internationalement reconnues et approuvées par de nombreux organismes d'accréditation, et les professionnels qui les obtiennent bénéficient donc 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 éditeur partenaire agréé (Licensed Partner Publisher LPP) 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 offrir la certification EBIOS Risk Manager Skills, et est agréé par la CNIL (Commission nationale de l'informatique et des libertés) pour offrir la certification DPO. Pour plus 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. Elles garantissent que les exigences de la norme ont été remplies et validées avec la cohérence, le professionnalisme et l'impartialité adéquats.

Un service orienté vers le client
Nous sommes une entreprise orientée vers le client et nous traitons tous nos clients avec estime, importance, professionnalisme et équité. 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 temps de réponse maximum de 24 heures sans compromettre la qualité des services.

Flexibilité et confort
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 permet de disposer de plus de temps libre, d'offrir davantage de possibilités d'avancement professionnel et de réduire les coûts.

Code de déontologie de PECB

Le code de déontologie représente les valeurs et l'éthique les plus élevées que PECB s'engage à respecter, car il en reconnaît l'importance lorsqu'il s'agit de fournir des services et d'attirer des clients.

La Division 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. En outre, la Division de la conformité insiste constamment 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 demandeurs, 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 encourage 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 mondiales au fil des ans et établi la réputation dont PECB jouit aujourd'hui.

PECB estime que des valeurs éthiques fortes sont essentielles pour avoir des relations saines et solides. Par conséquent, il est de la responsabilité première de PECB de s'assurer que les professionnels de PECB adoptent un comportement en totale conformité avec les principes et les valeurs de PECB.

Les professionnels de PECB sont chargés de :

1. Adopter un comportement professionnel dans la prestation de services en faisant preuve d'honnêteté, d'exactitude, d'équité et d'indépendance.
2. Agir à tout moment dans le cadre de leur prestation de 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 à d'autres normes professionnelles.
3. Démontrer et développer des compétences dans leurs domaines respectifs et s'efforcer de continuellement améliorer leurs compétences et leurs connaissances
4. Ne proposer que des services professionnels pour lesquels ils sont qualifiés et compétents, et informer correctement les clients de la nature des services proposés, y compris de toute préoccupation ou risque pertinent
5. Informer leur employeur ou client de tout intérêt commercial ou affiliation qui pourrait influencer ou altérer leur jugement
6. Préserver la confidentialité des informations relatives à tout employeur ou client, actuel ou ancien, pendant la prestation de services
7. Respecter 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 la contribution d'autrui
9. Ne pas communiquer intentionnellement des informations fausses ou falsifiées qui pourraient compromettre l'intégrité du processus d'évaluation d'un candidat à une certification PECB ou un programme de certification PECB

10. Ne pas se présenter à tort ou à travers comme des représentants de PECB sans licence appropriée ou utiliser abusivement le logo, les certifications ou les certificats de PECB.
11. Ne pas agir d'une manière qui pourrait nuire à la réputation de PECB, à ses certifications ou à ses programmes de certification.
12. Coopérer pleinement à l'enquête menée à la suite d'une prétendue violation du présent code de déontologie

Pour lire la version complète du code de déontologie de PECB, allez à Code de déontologie | PECB.

Introduction au formation Lead Cybersecurity Manager

Dans le paysage numérique actuel, les organisations sont confrontées à un nombre toujours croissant de cybermenaces qui peuvent mettre en péril leurs données sensibles, leurs opérations et leur réputation. En conséquence, elles emploient des responsables de la cybersécurité qui contribuent à assurer une protection contre ces menaces évolutives. Cette formation est conçue pour doter les futurs responsables de la cybersécurité des compétences, connaissances et stratégies essentielles nécessaires pour établir et superviser des programmes de cybersécurité efficaces. Tout au long de cette formation, les participants acquerront une connaissance approfondie des principes et des meilleures pratiques nécessaires pour naviguer dans le domaine complexe de la gestion de la cybersécurité et des responsabilités d'un responsable de la cybersécurité pour assurer la sécurité des informations dans le cyberespace.

Le titre « Certified Lead Cybersecurity Manager » désigne une certification professionnelle destinée aux personnes visant à démontrer leur compétence dans l'établissement et la gestion de programmes de cybersécurité et à aider les organisations à protéger leurs systèmes contre les menaces en constante évolution. Cette certification reconnue internationalement aidera les professionnels à débloquer des opportunités d'avancement de carrière et à atteindre leurs objectifs professionnels.

Les certifications de PECB ne sont pas une licence ou une simple adhésion. Elles attestent des connaissances et des compétences acquises grâce à nos formations et sont délivrées aux candidats possédant l'expérience requise et ayant réussi l'examen.

Le présent document spécifie le programme de certification PECB Lead Cybersecurity Manager conformément à la norme ISO/IEC 17024:2012. Il décrit également les mesures que les candidats doivent prendre pour obtenir et maintenir leurs qualifications. Il est donc très important que vous lisiez attentivement toutes les informations contenues dans ce document avant de remplir et de soumettre votre candidature. Si vous avez des questions ou avez besoin de plus amples informations après la lecture de ce document, veuillez contacter le bureau international de PECB à certification.team@pecb.com .

SECTION II : POLITIQUES ET RÈGLEMENTS RELATIFS À L'EXAMEN

Préparer et programmer 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 programmer l'examen, les candidats ont deux options :

1. Contacter 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 formation.
2. Passer un examen PECB à distance via l'application PECB Exams. Pour planifier un examen à distance, veuillez cliquer sur le lien suivant : 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.

Reprogrammer l'examen

Pour tout changement 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 : 1000 $ US[2]
- Examen Manager : 700 $ US
- Examen Foundation : 500 $ US
- Examen Transition : 500 $ US

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

Pour 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 maintien (FAM).

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

Domaines de compétence

L'objectif de l'examen « PECB Lead Cybersecurity Manager » est de s'assurer que le candidat a acquis les compétences nécessaires pour aider une organisation à établir et à gérer un programme de cybersécurité basé sur les meilleures pratiques du secteur.

La certification Lead Cybersecurity Manager s'adresse aux profils suivants :

- Responsables et dirigeants impliqués dans la gestion de la cybersécurité
- Personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité
- Professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité
- Professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes
- Cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité

Le contenu de l'examen est réparti comme suit :

- **Domaine 1 :** Concepts fondamentaux de la cybersécurité
- **Domaine 2 :** Lancement du programme de cybersécurité et de la gouvernance en matière de cybersécurité
- **Domaine 3 :** Définition des rôles et responsabilités en matière de cybersécurité et gestion des risques
- **Domaine 4 :** Sélection des contrôles de cybersécurité
- **Domaine 5 :** Mise en place de programmes de communication et de formation en matière de cybersécurité
- **Domaine 6 :** Intégration du programme de cybersécurité dans la gestion de la continuité d'activité et la gestion des incidents
- **Domaine 7 :** Évaluation des performances du programme de cybersécurité et amélioration continue de celui-ci

Domaine 1 : Concepts fondamentaux de la cybersécurité

Objectif principal : s'assurer que le candidat est capable d'expliquer les concepts fondamentaux de la cybersécurité.

Compétences	Énoncés de connaissances
1. Capacité à identifier les principales normes et les principaux cadres qui traitent de la cybersécurité	1. Connaissance de la famille de normes ISO/IEC 27000, du NIST Cybersecurity Framework et des publications NIST SP 800
2. Capacité à expliquer les principaux concepts de la cybersécurité, tels que le cyberespace et la cybercriminalité	2. Connaissance des définitions du cyberespace, de la cybercriminalité et de la sécurité de l'information, entre autres
3. Capacité à différencier la cybersécurité de la sécurité de l'information	3. Connaissance des différences entre la cybersécurité et la sécurité de l'information
4. Capacité à discuter des principaux éléments de la cybersécurité, tels que la sécurité du cloud, la sécurité du périmètre, la sécurité du réseau, la sécurité des points de terminaison, la sécurité des applications, la sécurité des données et la reprise après sinistre	4. Connaissance des principaux éléments de la cybersécurité, tels que la sécurité du cloud, la sécurité du périmètre, la sécurité du réseau, la sécurité des points de terminaison, la sécurité des applications, la sécurité des données et la reprise après sinistre
5. Capacité à expliquer les principes de sécurité de l'information : confidentialité, intégrité et disponibilité	5. Connaissance des définitions de la confidentialité, de l'intégrité et de la disponibilité des données
6. Capacité à expliquer la relation entre une vulnérabilité et une menace	6. Connaissance des notions de vulnérabilité et de menace
7. Capacité à définir les risques de sécurité de l'information	7. Connaissance de la définition du risque de sécurité de l'information
8. Capacité à classer les contrôles de sécurité par fonction et par type	8. Connaissance des types de contrôles de sécurité par fonction et par type

Domaine 2 : Lancement du programme de cybersécurité et de la gouvernance en matière de cybersécurité

Objectif principal : s'assurer que le candidat est capable d'amorcer la mise en œuvre d'un programme de cybersécurité et de l'aligner sur les meilleures pratiques du secteur.

Compétences	Énoncés de connaissances
1. Capacité à amorcer la mise en œuvre d'un programme de cybersécurité 2. Capacité à définir et appliquer différentes approches pour la mise en œuvre du programme de cybersécurité 3. Capacité à identifier les meilleures pratiques du secteur et à les intégrer dans le programme de cybersécurité 4. Capacité à distinguer la mission, les objectifs, les valeurs et les stratégies d'une organisation 5. Capacité à déterminer les objectifs de cybersécurité 6. Capacité à analyser l'environnement interne et externe d'une organisation, y compris les processus clés, les exigences commerciales et les parties intéressées pertinentes 7. Capacité à effectuer une analyse des écarts et à préparer un rapport d'analyse des écarts 8. Capacité à discuter des avantages du respect des meilleures pratiques en matière de cybersécurité 9. Capacité à expliquer la structure de la norme ISO/IEC 27032 et du NIST Cybersecurity Framework, et ce qui les différencie 10. Capacité à identifier des modèles de politique de cybersécurité et à établir et réviser la politique de cybersécurité	1. Connaissance des activités requises pour amorcer la mise en œuvre d'un programme de cybersécurité 2. Connaissance des approches de mise en œuvre des programmes de cybersécurité 3. Connaissance des meilleures pratiques du secteur pour la mise en œuvre du programme de cybersécurité 4. Connaissance des différences entre la mission, les objectifs, les valeurs et les stratégies d'une organisation 5. Connaissance des aspects à prendre en considération lors de la détermination des objectifs de cybersécurité 6. Connaissance des approches d'analyse de l'environnement interne et externe d'une organisation, y compris ses processus clés, ses exigences commerciales et les parties intéressées pertinentes 7. Connaissance des étapes à suivre pour effectuer une analyse des écarts et du contenu du rapport d'analyse des écarts 8. Connaissance des avantages du respect des meilleures pratiques en matière de cybersécurité 9. Connaissance des cadres de cybersécurité, tels que ISO/IEC TS 27110 et NIST Cybersecurity Framework 10. Connaissance du processus d'établissement et d'examen de la politique de cybersécurité et des modèles de politique de cybersécurité

Domaine 3 : Définition des rôles et responsabilités en matière de cybersécurité et gestion des risques

Objectif principal : s'assurer que le candidat est capable d'expliquer les rôles et responsabilités des parties prenantes en cybersécurité et de gérer les risques.

Compétences	Énoncés de connaissances
1. Capacité à expliquer les structures organisationnelles traditionnelles et autres de cybersécurité	1. Connaissance des structures organisationnelles traditionnelles et autres de cybersécurité
2. Capacité à expliquer le rôle des parties prenantes dans la mise en œuvre et l'amélioration d'un programme de cybersécurité	2. Connaissance des rôles et responsabilités des principales parties prenantes dans la mise en œuvre et l'amélioration d'un programme de cybersécurité
3. Capacité à expliquer les rôles et responsabilités du conseil d'administration, de la direction générale et du RSSI concernant le programme de cybersécurité	3. Connaissance des rôles et responsabilités du conseil d'administration, de la direction générale et du RSSI concernant le programme de cybersécurité
4. Capacité à expliquer le rôle et les responsabilités du responsable de la sécurité de l'information et du responsable de la cybersécurité	4. Connaissance des rôles et responsabilités du responsable de la sécurité de l'information et du responsable de la cybersécurité
5. Capacité à expliquer le système de gestion des actifs et la gestion des actifs	5. Connaissance de la relation entre le système de gestion des actifs et la gestion des actifs
6. Capacité à établir un programme de gestion des actifs de cybersécurité	6. Connaissance des principales étapes de la gestion des actifs dans le cyberespace
7. Capacité à différencier ISO 31000 et ISO/IEC 27005	7. Connaissance des différences entre ISO 31000 et ISO/IEC 27005
8. Capacité à évaluer, traiter et surveiller les risques	8. Connaissance des approches d'évaluation des risques, des stratégies de traitement des risques et des processus de surveillance et d'examen des risques

Domaine 4 : Sélection des contrôles de cybersécurité

Objectif principal : s'assurer que le candidat est capable d'identifier et d'expliquer les principales cybermenaces et leurs vecteurs d'atténuation, et de mettre en œuvre des contrôles clés de cybersécurité conformément aux meilleures pratiques.

Compétences	Énoncés de connaissances
1. Capacité à identifier et à décrire les vecteurs d'attaque courants 2. Capacité à identifier et à atténuer les attaques internes 3. Capacité à identifier et à atténuer les attaques externes 4. Capacité à mettre en œuvre des contrôles clés de cybersécurité, tels que des contrôles de sécurité des applications, des contrôles cryptographiques, des contrôles de gestion des vulnérabilités, des contrôles de gestion des points de terminaison et des changements, des contrôles contre les logiciels malveillants, des contrôles d'accès et des contrôles de gestion de réseau 5. Capacité à établir une protection de la vie privée sur Internet	1. Connaissance des vecteurs d'attaque courants 2. Connaissance des attaques internes et des stratégies pour les atténuer 3. Connaissance des types d'attaques externes (malware, ransomware, ingénierie sociale, menaces contre les données, déni de service, désinformation et mésinformation, menaces Internet et attaques de la chaîne d'approvisionnement) et des stratégies pour les atténuer 4. Connaissance des contrôles de sécurité des applications, des contrôles cryptographiques, des contrôles de gestion des vulnérabilités, des contrôles de gestion des points de terminaison et des changements, des contrôles contre les logiciels malveillants, des contrôles d'accès et des contrôles de gestion de réseau 5. Connaissance des pratiques visant à garantir la protection de la vie privée sur Internet, telles que la suppression des informations, l'anonymisation, la pseudonymisation, la prévention des fuites de données, la sauvegarde des informations et l'utilisation de modèles de services cloud

Domaine 5 : Mise en place de programmes de communication et de formation en matière de cybersécurité

Objectif principal : s'assurer que le candidat est capable d'établir un cadre de partage d'informations et un programme de développement des compétences qui répond aux besoins de l'organisation.

Compétences	Énoncés de connaissances
1. Capacité à expliquer l'importance d'établir un cadre de partage d'informations et de coordination en matière de cybersécurité 2. Capacité à identifier la communauté des réseaux de partage d'informations et de coordination 3. Capacité à catégoriser et classer les informations à partager 4. Capacité à établir des politiques, des procédures, des processus et des méthodes de partage d'informations et de coordination 5. Capacité à expliquer et définir les contrôles techniques et la normalisation du partage d'informations et de la coordination 6. Capacité à discuter des avantages des systèmes de test et à identifier les types de systèmes de test 7. Capacité à faire la différence entre formation et sensibilisation 8. Capacité à entreprendre des activités de formation et de sensibilisation dans le cadre des programmes de formation et de sensibilisation, respectivement	1. Connaissance des avantages de l'établissement d'un cadre de partage d'informations et de coordination en matière de cybersécurité 2. Connaissance des principales étapes à suivre pour identifier la communauté de partage d'informations et de coordination 3. Connaissance des principales activités de catégorisation et de classification des informations à partager 4. Connaissance des techniques et des meilleures pratiques pour établir des politiques, des procédures, des processus et des méthodes de partage d'informations et de coordination 5. Connaissance des principaux contrôles techniques et de la normalisation du partage d'informations et de la coordination 6. Connaissance des principaux avantages des systèmes de test et des types de systèmes de test, tels que les tests de performances, d'utilisabilité, de charge, de transgression, de migration, de fonctionnalité, d'évolutivité et de récupération 7. Connaissance de la différence entre la formation et la sensibilisation 8. Connaissance des étapes pour établir un programme de sensibilisation et mener des activités de sensibilisation, déterminer les besoins en matière de développement des compétences, établir un programme de développement des compétences et planifier, mener et évaluer les activités de développement des compétences

Domaine 6 : Intégration du programme de cybersécurité dans la gestion de la continuité d'activité et la gestion des incidents

Objectif principal : s'assurer que le candidat est capable d'intégrer le programme de cybersécurité dans le plan de gestion de la continuité d'activité et les processus de gestion des incidents de l'organisation.

Compétences	Énoncés de connaissances
1. Capacité à déterminer les objectifs de continuité d'activité 2. Capacité à discuter du rôle de la préparation des TIC pour la continuité d'activité (PTCA) dans la gestion de la continuité d'activité (GCA) 3. Capacité à déterminer les principes, les éléments et les phases de la PTCA 4. Capacité à planifier, préparer, détecter, signaler, communiquer et traiter les incidents de cybersécurité 5. Capacité à élaborer une politique et un plan de gestion des incidents de cybersécurité 6. Capacité à mesurer et à examiner la gestion des incidents	1. Connaissance des étapes à suivre pour déterminer les objectifs de continuité d'activité 2. Connaissance rôle de la PTCA dans la GCA 3. Connaissance des principes, éléments et phases de la PTCA 4. Connaissance des principales phases de la gestion des incidents, y compris la planification et la préparation, la détection et le signalement, l'évaluation et la prise de décision, la réponse aux incidents et l'apprentissage des leçons tirées des incidents 5. Connaissance du contenu de la politique et du plan de gestion des incidents de cybersécurité 6. Connaissance des étapes de mesure et d'examen de la gestion des incidents de cybersécurité

Domaine 7 : Évaluation des performances du programme de cybersécurité et amélioration continue de celui-ci

Objectif principal : s'assurer que le candidat est capable d'évaluer l'efficacité du programme de cybersécurité.

Compétences	Énoncés de connaissances
1. Capacité à déterminer les étapes et les techniques de tests de cybersécurité 2. Capacité à identifier et valider les faiblesses techniques sur la base du guide NIST SP 800-115 3. Capacité à préparer les tests et la documentation pour les tests 4. Capacité à mener des activités post-tests 5. Capacité à mesurer les performances du programme de cybersécurité, à déterminer les objectifs de mesure, à définir les aspects à surveiller et à mesurer, et à établir des indicateurs de performance 6. Capacité à améliorer continuellement le programme de cybersécurité	1. Connaissance des étapes et des techniques de test de cybersécurité, telles que les tests d'intrusion et l'évaluation de la vulnérabilité 2. Connaissance des recommandations NIST SP 800-115 pour identifier et valider les faiblesses techniques 3. Connaissance des processus de préparation et de documentation des tests 4. Connaissance des activités post-tests, telles que les rapports de tests et les recommandations d'atténuation 5. Connaissance des méthodes de surveillance, de mesure, d'analyse et d'évaluation du programme de cybersécurité 6. Connaissance des activités qui améliorent continuellement le programme de cybersécurité

Sur la base des domaines mentionnés ci-dessus et de leur pertinence, 80 questions à choix multiple 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	% des 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 compétence	Concepts fondamentaux de la cybersécurité	7	8,75	X	
	Lancement du programme de cybersécurité et de la gouvernance en matière de cybersécurité	10	12,5	X	
	Définition des rôles et responsabilités en matière de cybersécurité et gestion des risques	15	18,75	X	
	Sélection des contrôles de cybersécurité	20	25		X
	Mise en place de programmes de communication et de formation en matière de cybersécurité	8	10	X	
	Intégration du programme de cybersécurité dans la gestion de la continuité d'activité et la gestion des incidents	10	12,5		X
	Évaluation des performances du programme de cybersécurité et amélioration continue de celui-ci	10	12,5		X
	Total	**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 postuler pour l'obtention du titre « PECB Certified Lead Cybersecurity Manager ».

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 ; 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 : l'examen à choix multiple peut être utilisé pour évaluer la compréhension des candidats sur des concepts simples ou complexes. Il comprend à la fois des questions autonomes et basées sur un scénario. Les questions autonomes sont indépendantes de l'examen et ne dépendent pas du contexte, tandis que les questions basées sur un scénario dépendent du contexte,

c'est-à-dire qu'elles sont élaborées en fonction d'un scénario que le candidat doit lire et pour lequel il doit fournir des réponses à cinq questions liées à ce scénario. En répondant à des questions autonomes et basées sur un scénario, les candidats devront appliquer différents concepts et principes expliqués lors 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 une option de réponse correcte (réponse admise) et deux options de réponse incorrecte (distracteurs).

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

- 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

Un exemple de questions d'examen est fourni ci-dessous.

Remarque : 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 des informations spécifiques sur les types d'examens, les langues disponibles et d'autres détails, contactez examination.team@pecb.com ou consultez la Liste des examens PECB.

Exemples de questions d'examen

Blue9, une entreprise technologique de taille moyenne, propose une large gamme de services et de solutions, notamment le développement de logiciels, le cloud computing et l'analyse de données. Réputée pour ses pratiques innovantes et son dévouement aux solutions orientées client, l'entreprise s'est bâti une solide réputation dans ce secteur. Dans le paysage numérique actuel, où les cybermenaces peuvent avoir des conséquences importantes, *Blue9* a adopté une approche proactive pour assurer la sécurité et la fiabilité de ses systèmes en mettant en œuvre un programme complet de cybersécurité. L'approche qu'elle a utilisée pour la mise en œuvre du programme de cybersécurité impliquait une mise en œuvre globale des processus de cybersécurité, et non l'isolement de certains processus.

Le responsable de la sécurité de l'information (RSI) s'est vu confier la responsabilité d'assurer la mise en œuvre et la gestion opérationnelle des pratiques de cybersécurité de l'entreprise. Lors de la mise en œuvre du programme de cybersécurité, le RSI a entrepris une revue de la gouvernance de *Blue9* en matière de cybersécurité, laquelle reposait sur quatre principes : des rôles et des responsabilités clairs pour chaque département, une stratégie globale adaptée pour répondre aux besoins de l'entreprise, l'intégration de la cybersécurité dans les processus de gestion des risques existants et la planification de la réponse aux incidents de cybersécurité.

Le mois dernier, *l'équipe de sécurité des informations de Blue9* a détecté une activité inhabituelle sur le réseau de l'entreprise, ce qui a affecté plusieurs services incapables d'accéder à des informations cruciales. À l'aide d'un outil open source de « sniffing » de réseau et d'analyse de paquets, l'équipe a mené une enquête approfondie, identifié la source et la nature de l'activité et mis en œuvre rapidement des solutions temporaires pour restaurer les fonctionnalités normales du réseau.

De plus, afin de se préparer à des incidents similaires à l'avenir, l'entreprise a décidé de réévaluer ses procédures et politiques de réponse aux incidents. L'une des modifications apportées concernait l'autorité de l'équipe de réponse aux incidents (Incident Response Team, ou IRT) : à l'avenir, en cas d'incident, l'IRT serait uniquement chargée de fournir des conseils aux autres équipes sans avoir d'autorité sur elles. Selon la direction de l'entreprise, ce modèle favoriserait la collaboration plutôt que le commandement, garantissant ainsi que tous les services pourraient fonctionner de manière autonome tout en bénéficiant de l'expertise de l'IRT.

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

1. **Quelle approche *Blue9* a-t-elle adoptée pour mettre en œuvre le programme de cybersécurité ?**
   A. Approche systématique
   B. **Approche par systèmes**
   C. Approche intégrée

2. **Quel principe de sécurité des informations a été affecté en raison de l'impact de l'activité inhabituelle du réseau ?**
   A. Confidentialité
   B. Intégrité
   C. **Disponibilité**

3. **La gouvernance de *Blue9* en matière de cybersécurité repose sur quatre grands principes. Est-ce une bonne pratique à suivre ?**
   A. Oui, la gouvernance de *Blue9* en matière de cybersécurité suit tous les principes qui devraient être prioritaires pour garantir la sécurité
   B. **Non, les principes de gouvernance en matière de cybersécurité devraient également inclure la promotion d'une culture de cyber-résilience**
   C. Non, les principes de gouvernance en matière de cybersécurité ne devraient pas inclure l'intégration de la cybersécurité dans les processus de gestion des risques existants, car cela dépend de l'approche de mise en œuvre du programme de cybersécurité

4. **Le RSI s'est vu confier la responsabilité d'assurer la mise en œuvre et la gestion opérationnelle efficaces des pratiques de cybersécurité de *Blue9*. Est-ce acceptable ?**
   A. **Oui, le RSI est chargé d'assurer la réussite de la mise en œuvre des pratiques de cybersécurité et leur bonne gestion opérationnelle**
   B. Non, un RSI est responsable uniquement de la mise en œuvre des pratiques de cybersécurité mais pas de leur gestion opérationnelle
   C. Non, l'organisation doit nommer un responsable de la cybersécurité pour assurer la mise en œuvre et la gestion opérationnelle efficaces des pratiques de cybersécurité

5. ***Blue9* a confié à l'IRT la responsabilité de fournir des conseils aux autres équipes sans avoir d'autorité sur elles. Laquelle des structures suivantes de l'équipe de réponse aux incidents *Blue9* a-t-elle choisie dans ce cas ?**
   A. IRT centrale
   B. IRT distribuée
   C. **Équipe de coordination**

Politique de sécurité de l'examen

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 impartial de tous les candidats.

Toute divulgation d'informations sur le contenu des examens PECB constitue une violation directe de cette politique et du code de déontologie 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 au passage d'un examen 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 signalés à 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 de l'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. En outre, 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 correction, 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 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.

Résultats de l'examen

Les résultats de l'examen 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 dissertation et de deux à quatre semaines pour les examens à choix multiple sur papier.
- Pour les examens à choix multiple 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 au e-mail pour aider les candidats à mieux se préparer à une reprise.

Les candidats qui ne sont pas satisfaits des résultats peuvent demander une réévaluation en écrivant à dans examination.team@pecb.com les 30 jours suivant la date de réception des résultats. Les demandes de réévaluation reçues après 30 jours ne seront pas traitées. Si les candidats contestent les résultats de la réévaluation, ils disposent de 30 jours à compter de la date de réception des résultats de l'examen réévalué pour déposer une réclamation via le système de ticket de PECB. Les réclamations relatives à la certification reçues après 30 jours ne seront pas traitées.

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 première tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la tentative suivante (première reprise).

Remarque : 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 (les frais payés pour la formation comprennent une première tentative d'examen et une reprise). Sinon, des frais de reprise s'appliquent.

Aux 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.

SECTION III : PROCESSUS ET CONDITIONS DE CERTIFICATION

Certification PECB Lead Cybersecurity Manager

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

Les exigences des certifications du programme PECB Lead Cybersecurity Manager sont les suivantes :

Certification	Éducation	Examen	Expérience professionnelle	Expérience en projet de cybersécurité	Autres exigences
PECB Certified Provisional Cybersecurity Manager	Au moins l'enseignement secondaire	Examen PECB Certified Lead Cybersecurity Manager ou équivalent	Aucune	Aucune	Signature du Code de déontologie de PECB
PECB Certified Cybersecurity Manager		Examen PECB Certified Lead Cybersecurity Manager ou équivalent	Deux années : Un an d'expérience professionnelle en cybersécurité	Au moins 200 heures d'activité en cybersécurité	
PECB Certified Lead Cybersecurity Manager		Examen PECB Certified Lead Cybersecurity Manager ou équivalent	Cinq années : Deux ans d'expérience professionnelle en cybersécurité	Au moins 300 heures d'activité en cybersécurité	
PECB Certified Senior Lead Cybersecurity Manager		Examen PECB Certified Lead Cybersecurity Manager ou équivalent	Dix années : Sept ans d'expérience professionnelle en cybersécurité	Au moins 1 000 heures d'activité en cybersécurité	

Pour être considérées comme valides, les activités de cybersécurité doivent suivre les bonnes pratiques de gestion de la cybersécurité et inclure les éléments suivants :

1. Effectuer une analyse des écarts sur le programme de cybersécurité
2. Élaborer une politique de cybersécurité
3. Apprécier et traiter les risques liés à la cybersécurité
4. Mettre en œuvre des contrôles de cybersécurité
5. Évaluer les performances en matière de cybersécurité et en rendre compte

Demander la certification

Tout candidat ayant réussi l'examen (ou un équivalent accepté par PECB) est autorisé à demander le titre de compétences de PECB pour lequel il a été évalué. 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 références 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 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 :

- Enregistrez votre compte.
- Vérifiez vos e-mails pour activer le lien de confirmation.
- Connectez-vous 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 exigences de certification relatives au titre concerné. Le candidat recevra un courriel l'informant de l'état de sa candidature et de la décision de certification.

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 de l'insigne numérique, cliquez ici. PECB offre un soutien 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. Les références professionnelles doivent provenir de personnes ayant travaillé avec le candidat dans un environnement professionnel et pouvant ainsi attester de son expérience de management de la cybersécurité, 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 en projet de cybersécurité

Le journal de projet de cybersécurité 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 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 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 conduire à la rétrogradation du candidat à un titre inférieur.

SECTION IV : POLITIQUES DE CERTIFICATION

Refus de la certification

PECB peut refuser le programme de certification/certificat 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 réclamation dans le cadre de la procédure de réclamation et de recours. Pour des informations plus détaillées, reportez-vous à la section **Politique en matière de plainte et d'appel**.

Le paiement de la demande de 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 de PECB concernant le développement professionnel continu (DPC) et les frais annuels de maintien (FAM).

Suspendue

PECB peut suspendre temporairement la certification du candidat s'il ne satisfait pas aux exigences. 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.

Révoquée

PECB peut révoquer 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 de la 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 réclamation dans le cadre de la procédure de réclamation et de recours. Pour des informations plus détaillées, reportez-vous à la section **Politique en matière de plainte et d'appel**.

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 Options de statut de certification.

Mise à niveau et déclassement des titres de compétences

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, consulter 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 frais annuels de maintien (FAM) n'ont pas été payés.
- Les heures de développement professionnel continu (DPC) n'ont pas été soumises.
- Un nombre insuffisant d'heures de DPC a été soumis.
- La preuve des heures de DPC n'a pas été soumise sur demande.

Remarque : *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. Les détenteurs de certifications Master qui ne soumettent pas les heures de DPC et ne paient pas les FAM verront leurs certifications révoquées.*

Renouvellement de la certification
Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Pour les maintenir, 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). Par ailleurs, le paiement des frais annuels de maintien (120 $ US) est obligatoire. 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 douze mois, 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 à certification.team@pecb.com
et payer les frais requis.

Politique en matière de plainte et d’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 réclamation. Si la réponse de PECB n’est pas satisfaisante, le candidat a le droit de faire appel.

Pour plus d’informations, consultez la Politique en matière de plainte et d’appel ici.

SECTION V : POLITIQUES GÉNÉRALES DE PECB

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 pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective (par exemple, la certification Lead Cybersecurity Manager).

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[3] 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[4]. 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.*

Politique de comportement

PECB vise 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 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'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.

[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,
bureau 336 Montréal
QC H1S 0A5
CANADA

Tél./Fax :

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

E-mails

Examen :
examination.team@pecb.com

Certification :
certification.team@pecb.com

Service client :
customer@pecb.com

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.

www.pecb.com