PECB

BEYOND RECOGNITION

DIRECTIVE NIS 2 LEAD IMPLEMENTER

Manuel du candidat

PECB

Table des matières

SECTION I : INTRODUCTION **3**
À propos de PECB 3
Valeur de la certification PECB 4
Code de déontologie de PECB 5
Introduction à NIS 2 Directive Lead Implementer 7
SECTION II : POLITIQUES ET RÈGLEMENTS RELATIFS À L'EXAMEN DE PECB **8**
Préparer et programmer l'examen 8
Domaines de compétence 9
Passer l'examen 18
Politique de sécurité de l'examen 22
Résultats d'examen 23
Politique de reprise d'examen 23
SECTION III : PROCESSUS ET EXIGENCES DE CERTIFICATION **25**
PECB NIS 2 Directive 25
Demander la certification 26
Expérience professionnelle 26
Références professionnelles 26
Expérience de projet de cybersécurité 26
Évaluation des demandes de certification 27
SECTION IV : POLITIQUES DE CERTIFICATION **28**
Refus de la demande de certification 28
Options de statut de certification 28
Mise à niveau et déclassement des titres de compétences 29
Renouveler la certification 29
Fermeture d'un dossier 29
Plainte et appel 30
SECTION V : POLITIQUES GÉNÉRALES DE PECB **31**
Examens et certifications d'autres organismes de certification accrédités 31
Non-discrimination et aménagements spéciaux 31
Politique de comportement 31
Politique de remboursement 31

PECB

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui propose des services d'éducation[1] et de certification de personnes, 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 proposant de précieux programmes d'évaluation, de certification et de certificat par rapport aux normes internationalement reconnues.

Nos principaux objectifs sont :

1. Établir les exigences minimales nécessaires pour certifier les professionnels
2. Examiner et vérifier les qualifications des candidats pour s'assurer qu'ils sont éligibles à la certification
3. Maintenir et améliorer continuellement le processus d'évaluation des personnes certifiantes
4. Certifier les personnes qualifiées, accorder les désignations et maintenir les répertoires respectifs
5. Établir les exigences pour le renouvellement périodique de la certification et veiller au respect de ces exigences
6. S'assurer que les candidats respectent les normes éthiques dans leur pratique professionnelle
7. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification/programme de certificat auprès des organisations, des employeurs, des fonctionnaires, des praticiens dans des domaines connexes et auprès 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

Devenir la référence mondiale en matière de services de certification professionnelle et de programmes de certificat.

Nos valeurs

Intégrité, professionnalisme, équité

[1] Éducation fait référence aux formations développées par PECB, et offertes dans le monde entier par les Partenaires PECB.

Valeur de la certification PECB

Reconnaissance mondiale
Les titres de compétences PECB sont internationalement reconnus et approuvés par de nombreux organismes d'accréditation, de sorte que les professionnels qui les poursuivent bénéficieront de notre reconnaissance sur les marchés nationaux et internationaux.

La valeur des certifications 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) sous ISO/ IEC 17024 – Exigences générales pour les organismes procédant à la certification de personnes. La valeur des programmes de certificat PECB est validée par l'accréditation de l'ANSI National Accreditation Board (ANAB-Accreditation ID 1003) selon ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB est membre associé de l'Association indépendante des registraires accrédités (IAAR), membre à part entière de l'International Personnel Certification Association (IPC), membre signataire de l'IPC MLA et membre du Club EBIOS, CPD Certification Service, CLUSIF, Credential. Moteur et ITCC. De plus, PECB est un éditeur partenaire agréé (LPP) agréé par le Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) pour la norme Cybersecurity Maturity Model Certification (CMMC), et est approuvé 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 proposer la certification DPO. Pour des informations plus détaillées, cliquez ici.

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

Conformité aux normes
Nos certifications et programmes de certificats sont une démonstration de 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.

Service orienté client
Nous sommes une entreprise orientée sur 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 du service.

Flexibilité et commodité
Les opportunités d'apprentissage en ligne rendent votre parcours professionnel plus pratique car vous pouvez planifier vos sessions d'apprentissage en fonction de votre style de vie. Une telle flexibilité vous donne plus de temps libre, offre plus de possibilités d'avancement de carrière et réduit les coûts.

PECB

Code de déontologie de PECB

Le code d'éthique représente les valeurs et l'éthique les plus élevées que PECB s'engage pleinement à suivre, car il en reconnaît l'importance pour fournir des services et attirer des clients.

La Division Conformité s'assure que les employés, formateurs, examinateurs, surveillants, partenaires, distributeurs, membres de différents conseils et comités consultatifs de PECB, personnes certifiées et titulaires de certificats (ci-après « professionnels de PECB ») adhèrent à ce code d'éthique. En outre, la Division Conformité souligne systématiquement la nécessité de se comporter de manière professionnelle et en toute responsabilité, compétence et équité dans la prestation de services avec les parties prenantes internes et externes, telles que les demandeurs, les candidats, les personnes certifiées, les titulaires de certificat, les autorités d'accréditation et les autorités gouvernementales.

PECB est convaincu que pour parvenir au succès organisationnel, il doit pleinement comprendre les besoins et les attentes des clients et des parties prenantes. Pour ce faire, PECB favorise une culture basée sur les plus hauts niveaux d'intégrité, de professionnalisme et d'équité, qui sont également ses valeurs. Ces valeurs font partie intégrante de l'organisation et ont caractérisé la présence et la croissance mondiales au fil des années et ont établi la réputation dont jouit aujourd'hui PECB.

PECB estime que des valeurs éthiques fortes sont essentielles pour entretenir des relations saines et solides. Par conséquent, il est de la responsabilité principale de PECB de garantir que les professionnels de PECB affichent un comportement en totale conformité avec les principes et les valeurs de PECB.

Les professionnels de PECB sont tenus de :

1. Se comporter de manière professionnelle, avec honnêteté, exactitude, équité, responsabilité et indépendance
2. Agir en tout temps uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, en respectant les normes professionnelles et les techniques applicables tout en offrant des services professionnels
3. Maintenir leurs compétences dans leurs domaines respectifs et s'efforcer d'améliorer constamment leurs capacités professionnelles
4. Ne proposer que des services professionnels pour lesquels ils sont qualifiés et informer correctement les clients de la nature des services proposés, y compris de toute préoccupation ou risque pertinent
5. Informer chaque employeur ou client de tout intérêt commercial ou affiliation qui pourrait influencer leur jugement ou nuire à leur équité
6. Traiter de manière confidentielle et privée les informations obtenues dans le cadre des relations professionnelles et commerciales de tout employeur ou client, actuel ou ancien
7. Se conformer à toutes les lois et réglementations des juridictions dans lesquelles les activités professionnelles sont exercées
8. Respecter la propriété intellectuelle et la contribution d'autrui
9. Ne pas communiquer, intentionnellement ou non, des informations fausses ou falsifiées qui pourraient compromettre l'intégrité du processus d'évaluation d'un candidat à une certification/programme de certificat PECB
10. Ne pas se présenter faussement ou à tort comme des représentants de PECB sans licence appropriée ou utiliser à mauvais escient le logo, les certifications ou les certificats de PECB.

11. Ne pas agir d'une manière qui pourrait compromettre la réputation de PECB ou de ses certifications/programmes de certificat
12. Coopérer pleinement à l'enquête menée à la suite d'une prétendue violation du présent Code de déontologie

La version complète du Code de déontologie de PECB peut être téléchargée ici.

Introduction à NIS 2 Directive Lead Implementer

La directive NIS 2 précise les exigences visant à renforcer la sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union européenne (UE). Un programme de cybersécurité conforme aux exigences de la directive NIS 2 permet aux organisations de renforcer leurs mesures de cybersécurité, de protéger les infrastructures critiques et de se conformer aux exigences légales de l'UE. La directive NIS 2 s'applique à un large éventail d'organismes, définis comme entités essentielles ou importantes par la directive, avec des seuils de taille spécifiques pour chaque secteur, englobant celles qui fournissent des services essentiels ou importants à l'économie et à la société européennes, ainsi que les organisations qui sont les seuls fournisseurs d'un service critique dans un État membre.

Le titre « NIS 2 Directive Lead Implementer » est une certification professionnelle destinée aux personnes visant à démontrer leur compétence concernant les exigences de conformité de la directive NIS 2 et à diriger une équipe de mise en œuvre.

La mise en œuvre étant un métier très recherché, l'obtention d'une certification reconnue internationalement peut booster considérablement votre carrière et vous permettre d'atteindre vos objectifs professionnels.

Le présent document spécifie le programme de certificationPECB NIS 2 Directive Lead Implementer conformément à la norme ISO/IEC 17024:2012. Il décrit également les étapes que les candidats doivent suivre pour obtenir et conserver leurs titres de compétences. Il est très important que vous lisiez toutes les informations contenues dans ce manuel avant de remplir et de soumettre votre candidature. Si vous avez des questions après la lecture de ce document, veuillez, contactez le bureau international de PECB à l'adresse certification.team@pecb.com.

PECB

SECTION II : POLITIQUES ET RÈGLEMENTS RELATIFS À L'EXAMEN DE PECB

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 tenus de suivre la formation pour pouvoir passer l'examen, leur participation peut augmenter considérablement leurs chances de réussir l'examen.

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

1. Contacter l'un de nos revendeurs qui proposent des sessions de formation et d'examen. Les candidats trouveront un Revendeur de formations dans une région donnée sur la page Active Partners. Le calendrier des sessions de formation PECB est également disponible sous l'onglet Training Events.
2. Passer un examen PECB à distance de chez eux ou de n'importe quel endroit qu'ils préfèrent grâce à l'application PECB Exams, qui est accessible ici : PECB Exams application. Pour planifier un examen à distance, veuillez consulter 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

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

- Examen Lead : 1000 $ US[1]
- Examen Manager : 700 $ US
- Examen Foundation : 500 $ US
- Examen Transition : 500 $ US

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

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

Domaines de compétence

L’examen « PECB NIS 2 Directive Lead Implementer » a pour objectif de veiller à ce que le candidat acquiert les compétences nécessaires pour aider un organisme à établir, mettre en œuvre, gérer et maintenir un programme de conformité à la directive NIS 2.

La certification NIS 2 Directive Lead Implementer est destinée aux :

- Professionnels de la cybersécurité cherchant à acquérir une compréhension approfondie des exigences de la directive NIS 2 et à apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes.
- Responsables informatiques et professionnels souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés et améliorer la résilience des systèmes critiques.
- Responsables gouvernementaux et réglementaires chargés de faire appliquer la directive NIS 2

Le contenu de l'examen est réparti comme suit :

- **Domaine 1 :** Concepts fondamentaux et définitions de la directive NIS 2
- **Domaine 2 :** Planification de la mise en œuvre des exigences de la directive NIS 2
- **Domaine 3 :** Rôles et responsabilités en matière de cybersécurité et gestion des risques
- **Domaine 4 :** Contrôles de cybersécurité, gestion des incidents et gestion des crises
- **Domaine 5 :** Communication et sensibilisation
- **Domaine 6 :** Test et surveillance d'un programme de cybersécurité

Domaine 1 : Concepts fondamentaux et définitions de la directive NIS 2

Objectif principal : S'assurer que le candidat est en mesure d'interpréter les concepts et les définitions de la directive NIS 2.

Compétences	Énoncés de connaissances
1. Capacité à expliquer les principaux concepts liés à la directive NIS 2 2. Capacité à développer une connaissance complète des normes ISO liées à la sécurité de l'information 3. Capacité à identifier d'autres bonnes pratiques de cybersécurité du secteur, y compris le cadre de cybersécurité du NIST et les contrôles CIS 4. Capacité à identifier les publications de l'ENISA pour la cybersécurité 5. Possibilité de comparer la directive NIS 2 avec son prédécesseur, la directive NIS 6. Capacité à analyser la structure, les objectifs et le sujet de la directive NIS 2 7. Capacité à évaluer l'impact potentiel de la directive NIS 2 sur diverses parties prenantes, y compris les entités essentielles et importantes 8. Capacité à décrire les amendes administratives associées au non-respect de la directive NIS 2 9. Capacité à reconnaître et à décrire les organismes importants de l'UE impliqués dans l'application et la réglementation de la cybersécurité au sein de l'Union européenne	1. Connaissance des principaux concepts et terminologies de la directive NIS 2 2. Connaissance des normes ISO liées à la sécurité de l'information, notamment ISO/IEC 27001 et ISO/IEC 27002. 3. Connaissance des cadres juridiques et des réglementations pertinentes en matière de sécurité de l'information et de cybersécurité, notamment la loi sur les marchés numériques, la loi sur les services numériques, la loi sur la résilience opérationnelle numérique, la loi de l'UE sur la cybersécurité, la loi européenne sur la cyber-résilience, la loi sur la gouvernance des données, le RGPD et la directive sur les services de paiement 2. 4. Connaissance du champ d'application de la directive NIS 2 et de sa comparaison avec la directive NIS 5. Connaissance de la relation entre la directive NIS 2 et la série ISO/IEC 27000 6. Connaissance de la structure, des objectifs et du sujet de la directive NIS 2 et de ses implications pour les organismes et les secteurs des infrastructures critiques 7. Connaissance de l'impact de la directive NIS 2 8. Connaissance des amendes administratives liées au non-respect de la directive NIS 2 et des critères de détermination de ces amendes 9. Connaissance des principales organisations de l'UE responsables de la gouvernance, de la réglementation et de la surveillance de la cybersécurité, ainsi que de leurs rôles dans l'application de la directive NIS 2.

Domaine 2 : Planification de la mise en œuvre des exigences de la directive NIS 2

Objectif principal : S'assurer que le candidat est en mesure d'identifier et d'expliquer les principales exigences de la directive NIS 2 et de planifier leur mise en œuvre.

Compétences	Énoncés de connaissances
1. Capacité à expliquer les composantes de la directive NIS 2, y compris la gouvernance, la gestion des crises, les mesures de risque et les obligations de déclaration 2. Capacité à définir l'approche de mise en œuvre des exigences de la directive NIS 2 3. Capacité à collecter, analyser et interpréter les informations nécessaires pour planifier la mise en œuvre des exigences de la directive NIS 2 4. Capacité à interpréter et à définir les objectifs de conformité à la directive NIS 2 5. Analyser et prendre en compte le contexte interne et externe d'une organisation 6. Capacité à identifier les rôles et responsabilités des principales parties intéressées pendant et après la mise en œuvre des exigences de la directive NIS 2 7. Capacité à effectuer une analyse des écarts et à clarifier les objectifs de conformité à la directive NIS 2 8. Capacité à définir et justifier le périmètre du programme de mise en œuvre de la directive NIS 2 adaptée aux objectifs spécifiques de conformité de la directive NIS 2 de l'organisation. 9. Capacité à expliquer les exigences de la directive NIS 2 liées à la gouvernance et à la stratégie de cybersécurité 10. Capacité à développer un programme de conformité en cybersécurité 11. Capacité à identifier les types de politiques et à établir une politique de cybersécurité	1. Connaissance des composants et des exigences de la directive NIS 2, y compris les définitions, la gouvernance, la gestion des crises, la gestion des risques et les obligations de reporting. 2. Connaissance des principales approches et méthodologies utilisées pour mettre en œuvre les exigences de la directive NIS 2 3. Connaissance des objectifs typiques de conformité à la directive NIS 2 et de la manière de les atteindre 4. Connaissance de ce qui constitue typiquement le contexte interne et externe d'une organisation 5. Connaissance des approches utilisées pour comprendre le contexte d'une organisation 6. Connaissance des techniques utilisées pour recueillir des informations sur une organisation et effectuer une analyse des écarts 7. Connaissance d'un plan de projet de mise en œuvre de la directive NIS 2 et d'une équipe de projet de mise en œuvre de la directive NIS 2 8. Connaissance des principales structures organisationnelles applicables à une organisation pour gérer la mise en œuvre de la directive NIS 2 9. Connaissance des caractéristiques du champ d'application de la directive NIS 2 en termes de limites organisationnelles, technologiques et physiques 10. Connaissance des articles de la directive NIS 2 qui traitent de la gouvernance et de la stratégie nationale de cybersécurité 11. Connaissance des activités nécessaires à l'élaboration d'un programme de conformité en cybersécurité

	12. Connaissance des bonnes pratiques et techniques utilisées pour rédiger et établir des politiques et procédures de cybersécurité

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

Objectif principal : S'assurer que le candidat est capable de définir les rôles et responsabilités en matière de cybersécurité et de gérer les risques.

Compétences	Énoncés de connaissances
1. Capacité à analyser la structure organisationnelle et à attribuer des rôles et responsabilités clés liés à la cybersécurité	1. Connaissance de la structure organisationnelle
2. Capacité à définir les rôles et les responsabilités au sein de l'organisation	2. Connaissance des rôles et responsabilités liés à la cybersécurité
3. Capacité à constituer une équipe de cybersécurité efficace au sein de l'organisme	3. Connaissance des exigences de la directive NIS 2 concernant la gestion d'actifs
4. Capacité à gérer efficacement les actifs de cybersécurité	4. Connaissance de la gestion des actifs de cybersécurité
5. Capacité à identifier les risques de cybersécurité en évaluant les menaces, les vulnérabilités et les impacts potentiels	5. Connaissance des exigences de la directive NIS 2 concernant la gestion des risques
6. Capacité à analyser les risques de cybersécurité pour déterminer leur probabilité et leurs conséquences potentielles	6. Connaissance des lignes directrices sur la gestion des risques, telles que les publications ISO 31000, ISO/IEC 27005 et ENISA
7. Capacité à évaluer les risques de cybersécurité pour les hiérarchiser en fonction de leur importance et de leur impact potentiel sur l'organisme	7. Connaissance de l'identification et de l'analyse des risques de cybersécurité pour déterminer la probabilité et les conséquences potentielles
8. Capacité à mettre en œuvre des stratégies de traitement des risques pour atténuer les risques de cybersécurité identifiés	8. Connaissance de l'évaluation des risques de cybersécurité pour mettre en œuvre des stratégies efficaces de traitement des risques
9. Capacité à communiquer et à consulter efficacement les parties prenantes concernées concernant les risques de cybersécurité et les stratégies d'atténuation	9. Connaissance de la communication et de la consultation des parties prenantes concernées concernant les risques de cybersécurité
10. Capacité à tenir des registres et à rendre compte des risques de cybersécurité, ainsi qu'à surveiller et examiner en permanence l'efficacité des efforts de gestion des risques de cybersécurité.	10. Connaissance de la tenue des dossiers et des rapports sur les risques de cybersécurité, les traitements et leur statut
	11. Connaissance de la surveillance et de la revue de la procédure pour déterminer l'efficacité des efforts de gestion des risques de cybersécurité

Domaine 4 : Contrôles de cybersécurité, gestion des incidents et gestion des crises

Objectif principal : S'assurer que le candidat est en mesure de mettre en œuvre les processus de cybersécurité requis pour la conformité à la directive NIS 2, y compris les contrôles de cybersécurité, la sécurité de la chaîne d'approvisionnement, la gestion des incidents et la gestion des crises.

Compétences	Énoncés de connaissances
1. Capacité à interpréter les exigences de la directive NIS 2 concernant les mesures de gestion des risques de cybersécurité 2. Capacité à expliquer les mesures de sécurité des ressources humaines en fonction des bonnes pratiques de l'industrie 3. Capacité à expliquer les bonnes pratiques pour un contrôle d'accès efficace afin de protéger les réseaux et les systèmes d'information 4. Capacité à utiliser des techniques de cryptographie pour améliorer la sécurité des données 5. Capacité à identifier et à mettre en œuvre les mesures nécessaires pour protéger les services et systèmes réseau 6. Capacité à sélectionner et à mettre en œuvre des processus de gestion des risques de la chaîne d'approvisionnement, à établir des processus de gestion des vulnérabilités et à améliorer la sécurité des informations dans les relations avec les fournisseurs. 7. Capacité à se préparer, détecter, signaler, évaluer, répondre et tirer des leçons des incidents de cybersécurité 8. Capacité à créer un plan de gestion de crise, des plans de communication de crise et des systèmes de communication d'urgence pour faire face à des situations difficiles 9. Capacité à élaborer des plans complets de continuité d'activité et des plans de reprise après sinistre pour assurer la continuité opérationnelle	1. Connaissance des exigences de la directive NIS 2 concernant les mesures techniques, opérationnelles et organisationnelles 2. Connaissance des contrôles de cybersécurité nécessaires à la gestion des risques, tels que la sécurité des ressources humaines, les contrôles d'accès, la cryptographie et la sécurité des réseaux 3. Connaissance des exigences de la directive NIS 2 qui traitent des mesures visant à garantir la sécurité de la chaîne d'approvisionnement 4. Connaissance des pratiques de gestion des risques de la chaîne d'approvisionnement, de gestion des vulnérabilités et de sécurité de l'information dans les relations avec les fournisseurs. 5. Connaissance des processus de préparation, de détection, de signalement, d'évaluation, de réponse et d'apprentissage des incidents de cybersécurité 6. Connaissance du rôle et des responsabilités des CSIRT dans le processus de gestion des incidents tel que défini par la directive NIS 2 7. Connaissance des obligations de déclaration d'incident imposées par la directive NIS 2 pour les parties impliquées dans la gestion des incidents 8. Connaissance des exigences de la directive NIS 2 pour les États membres et les CSIRT en matière de gestion des cyber-crises 9. Connaissance de la gestion de crise et des caractéristiques et de l'importance de la communication de crise 10. Connaissance de la gestion de la continuité d'activité, y compris les stratégies et la planification de la reprise

Domaine 5 : Communication et sensibilisation

Objectif principal : S'assurer que le candidat est en mesure de développer et de mettre en œuvre des programmes efficaces de communication, de développement des compétences et de sensibilisation pour soutenir la cybersécurité et les objectifs organisationnels et se conformer aux exigences de la directive NIS 2.

Compétences	Énoncés de connaissances
1. Capacité à planifier et à proposer des activités de développement des compétences, y compris des programmes de formation et de sensibilisation 2. Capacité à définir la structure et le type de programmes de développement des compétences alignés sur les objectifs organisationnels 3. Capacité à dispenser efficacement des programmes de formation et de sensibilisation pour répondre aux besoins identifiés 4. Capacité à apprécier les résultats et l'efficacité des programmes de formation et de sensibilisation 5. Capacité à planifier, exécuter et évaluer des activités de communication pour atteindre les objectifs de communication 6. Capacité à identifier les exigences de la directive NIS 2 concernant la sensibilisation à la cybersécurité et le partage d'informations 7. Capacité à appliquer les principes d'une stratégie de communication efficace	1. Connaissance des exigences de la directive NIS 2 pour la sensibilisation à la cybersécurité dans toute l'Union européenne 2. Connaissance des activités et des programmes de développement des compétences 3. Connaissance de la conception de programmes de compétences pour atteindre les objectifs organisationnels 4. Connaissance du processus de prestation de programmes de formation et de sensibilisation efficaces 5. Connaissance de l'évaluation des résultats et de l'efficacité des programmes de formation et de sensibilisation 6. Connaissance de la communication stratégique et de ses principes : transparence, pertinence, crédibilité, réactivité et clarté 7. Connaissance des stratégies de communication efficaces 8. Connaissance des accords de partage d'informations sur la cybersécurité et de la notification volontaire des informations pertinentes telles que définies dans la directive NIS 2

Domaine 6 : Test et surveillance d'un programme de cybersécurité

Objectif principal : S'assurer que le candidat est en mesure d'auditer, de mesurer, de surveiller et d'améliorer continuellement un programme de cybersécurité conformément à la directive NIS 2.

Compétences	Énoncés de connaissances
1. Capacité à comprendre et à expliquer les tests de cybersécurité	1. Connaissance des techniques de tests de cybersécurité
2. Capacité à identifier les exigences de la directive NIS 2 concernant les audits de sécurité et les auto-évaluations	2. Connaissance des exigences de la directive NIS 2 concernant les auto-évaluations et du rôle d'une telle évaluation pour garantir la conformité de la directive NIS 2
3. Capacité à réaliser des audits internes, à traiter les non-conformités et à comprendre les principes fondamentaux de l'audit	3. Connaissance de l'audit de conformité interne et des activités d'audit interne
4. Capacité à effectuer des auto-évaluations à l'aide de cadres tels que le cadre d'auto-évaluation de l'ENISA	4. Connaissance du cadre d'auto-évaluation de l'ENISA et d'autres outils d'évaluation de la cybersécurité
5. Capacité à définir des objectifs de mesure, à établir des indicateurs de performance et à déterminer des méthodes de suivi	5. Connaissance des objectifs de mesure, des indicateurs de performance et des méthodes de surveillance pour évaluer l'efficacité des programmes de cybersécurité
6. Capacité à identifier le rôle des CSIRT et des autorités compétentes dans la surveillance des cybermenaces tel que défini par la directive NIS 2	6. Connaissance des exigences de la directive NIS 2 pour les CSIRT sur la surveillance et l'analyse des menaces, des vulnérabilités et des incidents au niveau national.
7. Capacité à déterminer ce qui doit être surveillé, à rendre compte efficacement des résultats de la surveillance et à sélectionner les méthodes de surveillance appropriées	7. Connaissance de la communication des résultats de la surveillance aux parties prenantes et de la sélection des méthodes de surveillance appropriées
8. Capacité à surveiller les facteurs de changement, à maintenir et à améliorer les mesures de cybersécurité et à documenter les améliorations	8. Connaissance des facteurs de changement de la surveillance, du maintien et de l'amélioration des mesures de cybersécurité et de la documentation des améliorations

Sur la base des domaines mentionnés ci-dessus et de leur pertinence, l'examen contient 80 questions à choix multiples, résumées dans le tableau ci-dessous :

				Niveau de compréhension (Cognitif/Taxonomique) requis	
		Nombre de questions/points par domaine de compétence	%/points de l'examen consacré à chaque domaine de compétence	Questions qui mesurent la compréhension, l'application et l'analyse	Questions qui mesurent l'évaluation
Domaines de compétence	Concepts fondamentaux et définitions de la directive NIS 2	10	12.5	X	
	Planification de la mise en œuvre des exigences de la directive NIS 2	20	25	X	
	Rôles et responsabilités en matière de cybersécurité et gestion des risques	15	18.75		X
	Contrôles de cybersécurité, gestion des incidents et gestion des crises	15	18.75		X
	Communication et sensibilisation	10	12.5	X	
	Test et surveillance d'un programme de cybersécurité	10	12.5		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 la certification « PECB Certified NIS 2 Directive Lead Implementer » en fonction de leur niveau d'expérience.

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

Pour des informations plus détaillées sur les examens 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 d'un candidat sur de nombreux sujets, y compris des concepts simples ou complexes. Il comprend à la fois des questions autonomes et basées sur des scénarios. 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 des mises en situation, 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 multiples comporte trois options, dont l'une est l'option de réponse correcte (réponse saisie) 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 :

- Copie papier de la directive NIS 2
- 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 sera 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, consultez la Liste des examens PECB.

Exemples de questions d'examen

TechLink, une société multinationale, se spécialise dans la fourniture d'une large gamme de services de cloud computing adaptés aux secteurs de la finance et de la santé. Ses services permettent aux organisations d'exploiter tout le potentiel de la technologie cloud, de stimuler la transformation numérique et d'améliorer les services publics à l'échelle mondiale.

Opérant au sein de l'Union européenne, TechLink relève du cadre réglementaire de la directive NIS 2 en tant qu'entité essentielle. TechLink n'avait pas encore mis en œuvre les garanties nécessaires pour protéger correctement ses réseaux et systèmes et garantir le respect de la directive ; c'est pourquoi il a lancé un programme complet de cybersécurité. L'entreprise a adopté une approche qui lui a permis d'établir des normes de production élevées sans prescrire de méthodes spécifiques, ce qui lui a permis de trouver des moyens efficaces et innovants pour répondre à ces normes.

Conformément à l'article 21 de la directive NIS 2, l'entreprise a développé une stratégie de gestion de la continuité d'activité (BCM). Son approche pour développer la stratégie BCM impliquait une configuration de récupération contractuelle avec un tiers pour rechercher un soutien externe pour rétablir les processus clés, ainsi qu'une option de modification clé pour ajuster les processus opérationnels dans des circonstances de ressources limitées. Cette approche a facilité une réponse agile aux incidents, en équilibrant le support externe avec des ajustements internes pour accélérer le processus de récupération tout en répondant aux principales préoccupations de gestion telles que l'étendue de la planification, les coûts de mise en œuvre et les accords contractuels avec des fournisseurs tiers.

Dans le cadre du programme de cybersécurité, TechLink s'est concentré sur la garantie de la sécurité des réseaux et des systèmes d'information en favorisant une culture de gestion des risques, y compris l'évaluation des risques et la mise en œuvre de mesures de cybersécurité. Conformément à la directive NIS 2, ces mesures ont été approuvées par l'instance de direction de l'entreprise. L'instance de direction est rompue aux pratiques générales de gestion des risques, tandis que la société a jugé inutile de dispenser une formation complémentaire sur la gestion des risques de cybersécurité, l'un des membres possédant une expertise en matière de cybersécurité.

Récemment, TechLink a été confronté à un grave incident de cybersécurité au cours duquel une cyberattaque sophistiquée a ciblé ses systèmes critiques, entraînant une violation des données sensibles des clients. Cet incident a été l'occasion de démontrer son engagement à se conformer à la directive NIS 2. L'entreprise a isolé les systèmes concernés et a contenu l'intrusion pour éviter d'autres dommages. Ensuite, elle a rapidement informé les autorités compétentes, y compris le gouvernement national, dans les 24 heures suivant la détection. L'entreprise a également communiqué avec les clients concernés, leur fournissant des informations sur l'incident et les mesures à prendre pour protéger les données. L'entreprise a soumis un rapport final comprenant une description détaillée, le type de menace, les mesures d'atténuation appliquées et en cours, ainsi que l'impact transfrontalier.

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

1. **Quelles sanctions potentielles TechLink pourrait-il encourir en cas de non-respect de la directive NIS 2 ?**
   A. 7 millions d'euros soit 1,4% du chiffre d'affaires mondial annuel total
   B. **10 millions d'euros soit 2% du chiffre d'affaires mondial annuel total**
   C. 5 millions d'euros ou 1% du chiffre d'affaires mondial annuel total

2. **Quelle exigence de la directive NIS 2 TechLink a-t-il négligée ?**
   A. **Former les membres de l'organe de direction aux pratiques de gestion des risques de cybersécurité**
   B. Assurer l'approbation des mesures de cybersécurité par les groupes de résilience des entités critiques
   C. Créer un organe de direction composé de cinq membres possédant une vaste expérience en matière de cybersécurité

3. **Quelle approche réglementaire TechLink a-t-elle adoptée pour se conformer à la directive NIS 2 ?**
   A. Commander et contrôler
   B. **Basée sur la performance**
   C. Basée sur la gestion

4. **Compte tenu des mesures prises par TechLink en réponse à la cyberattaque sur ses systèmes critiques, à quel aspect de l'obligation de déclaration d'incident décrite à l'article 23 de la directive NIS 2 TechLink n'a-t-elle pas respecté ?**
   A. **Soumettre une mise à jour de statut intermédiaire sur demande**
   B. Fournir à l'ENISA un rapport de synthèse sur un incident significatif
   C. Soumettre une divulgation publique de l'incident dans les 48 heures suivant sa détection

5. **Quelle approche TechLink a-t-elle utilisée pour développer la stratégie GCA ?**
   A. Opération multisites
   B. Disposition de sauvegarde
   C. **Disposition combinée**

Politique de sécurité de l'examen

PECB s'engage à protéger l'intégrité de ses examens et du processus d'examen dans son ensemble, et s'appuie sur le comportement éthique des candidats, des candidats potentiels, des candidats et des partenaires pour maintenir la confidentialité des examens 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 PECB constitue une violation directe de cette politique et du Code de déontologie de PECB. Par conséquent, les candidats qui passent un examen PECB sont tenus de signer un accord de confidentialité et de non-divulgation de l'examen et doivent se conformer aux éléments suivants :

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

Une fois qu'un candidat prend connaissance ou a déjà connaissance des irrégularités ou des violations des points mentionnés ci-dessus, il est responsable de s'y conformer, sinon si de telles irrégularités devaient se produire, les candidats seront signalés directement à PECB ou s'ils constatent de telles irrégularités, ils doivent immédiatement se présenter au PECB.

Les candidats sont seuls responsables de comprendre et de respecter les règles et politiques de l'examen PECB, l'accord de confidentialité et de non-divulgation et le code d'éthique. Par conséquent, si une violation d'une ou plusieurs règles est identifiée, 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 des candidats à repasser un 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 un préjudice irréparable qu'aucun recours 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 contre les personnes qui enfreignent les règles et politiques, notamment en leur interdisant de manière permanente de rechercher des informations d'identification PECB et en révoquant

toutes les précédentes. 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 d'examen

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

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

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

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

Les candidats en désaccord avec les résultats peuvent demander une réévaluation en écrivant à examination.team@pecb.com dans 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 le PECB Ticketing System. Toute réclamation 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 le candidat échoue à l'examen à la 1re tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la tentative suivante (1re reprise).

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

Pour les 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.

PECB

SECTION III : PROCESSUS ET EXIGENCES DE CERTIFICATION

PECB NIS 2 Directive

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

Les certifications du groupe PECB NIS 2 Directive ont les exigences suivantes :

Titre de compétence	Éducation	Examen	Expérience professionnelle	Expérience de projet SM	Autres exigences
PECB Certified NIS 2 Directive Provisional Implementer	Au moins un enseignement secondaire	Examen PECB Certified NIS 2 Directive Lead Implementer ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified NIS 2 Directive Lead Implementer			Deux années : Un an d'expérience professionnelle dans la gestion de la cybersécurité	Les activités du projet: Total de 200 heures	
PECB Certified NIS 2 Directive Lead Implementer			Cinq années : Deux ans d'expérience professionnelle dans la gestion de la cybersécurité	Les activités du projet: Total de 300 heures	
PECB Certified NIS 2 Directive Senior Lead Implementer			Dix années : Sept ans d'expérience professionnelle dans la gestion de la cybersécurité	Les activités du projet: Total de 1 000 heures	

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

1. Réaliser des évaluations complètes des risques spécifiques aux systèmes d'infrastructures critiques
2. Gérer des plans de réponse aux incidents adaptés aux exigences de la directive NIS 2
3. Mise en œuvre d'actions et de mesures de sécurité appropriés
4. Mise en place de métriques et indicateurs de performance
5. Gérer et répondre aux incidents de cybersécurité
6. Réaliser des revues de direction
7. Gérer une équipe de cybersécurité

Demander la certification

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

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

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

Pour plus d'informations sur les étapes de demande de la 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 e-mail concernant l'état de sa candidature, y compris la décision de certification.

Suite à l'approbation du dossier par le Service 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 la réclamation du badge 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 de projet de cybersécurité

Le journal de projet 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 du candidat à la certification/programme de certificat. 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 l'intervalle requis, le service de certification validera la demande sur la base des informations initiales fournies, ce qui peut éventuellement conduire à la rétrogradation du candidat à une certification inférieure.

SECTION IV : POLITIQUES DE CERTIFICATION

Refus de la demande de certification

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

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

Les candidats dont la certification/le programme de certificat a été refusé peuvent déposer une plainte via la procédure de plainte et d'appel. Pour des informations plus détaillées, reportez-vous à la section Politique relative aux plaintes et aux appels.

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

Options de statut de certification

Active

Signifie que votre certification est en règle et valide, et qu'elle est maintenue en remplissant les exigences de PECB concernant le CPD et l'FAM.

Suspendue

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

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

Révocation de la certification

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

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

Les candidats dont la certification a été révoquée peuvent déposer une plainte via la procédure de plainte et d'appel. Pour des informations plus détaillées, reportez-vous à la section Politique relative aux plaintes et aux appels.

Autres statuts
En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour en savoir plus sur ces statuts et le statut de cessation définitive, rendez-vous sur 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, visiter l'onglet Mes certifications et cliquer sur le lien Mise à niveau. Les frais de demande de mise à niveau sont de 100 $ US.

Déclassement des titres de compétences
Une certification PECB peut être déclassée à un titre inférieur pour les raisons suivantes :
- Les FAM n'ont pas été payés.
- Les heures de FPC n'ont pas été soumises.
- Un nombre insuffisant d'heures de FPC a été soumis.
- La preuve des heures de FPC n'a pas été soumise sur demande.

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. D'autre part, les détenteurs de certifications Master qui ne soumettent pas les FPC et ne paient pas les FAM verront leurs certifications révoquées.*

Renouveler la certification
Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Pour les conserver, les professionnels certifiés PECB doivent répondre aux exigences liées au titre désigné, par exemple, ils doivent remplir le nombre requis d'heures de développement professionnel continu (DPC) De plus, ils doivent payer les frais de maintenance annuels (120 $). 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 un délai de un an, son dossier sera fermé. Toutefois, même si la période de certification expire, le candidat a le droit de rouvrir son dossier. Cependant, PECB ne sera plus responsable de tout changement concernant les conditions, les normes, les politiques et le Manuel du candidat qui étaient applicables avant la fermeture du dossier. Un candidat qui demande la réouverture de son dossier doit le faire par écrit et payer les frais requis.

Plainte et appel

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

Pour plus d'informations, consultez la Politique de plainte et d'appel de PECB ici..

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 ISO/IEC 27001 Lead Auditor).

Non-discrimination et aménagements spéciaux

Toutes les candidatures seront évaluées objectivement, sans considération d'âge, de sexe, de race, de religion, de nationalité ou d'état civil du candidat.

Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB fera des aménagements raisonnables [2]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[3]. 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 au bénéfice de ses parties prenantes externes : distributeurs, partenaires, formateurs, surveillants, examinateurs, membres de différents comités et conseils consultatifs, et clients (stagiaires, candidats, personnes certifiées et titulaires de certificats), ainsi que de créer et de maintenir un environnement de travail positif qui garantit la sécurité et le bien-être de son personnel et tient en haute estime la dignité, le respect et les droits de l'homme de son personnel.

L'objectif de cette politique est de garantir que PECB gère les comportements inacceptables des parties prenantes externes à l'égard du personnel de PECB de manière impartiale, confidentielle, équitable et en temps opportun. Pour lire la politique comportementale, cliquez ici..

Politique de remboursement

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

---

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

[3]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

Tel./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

©2023 PECB