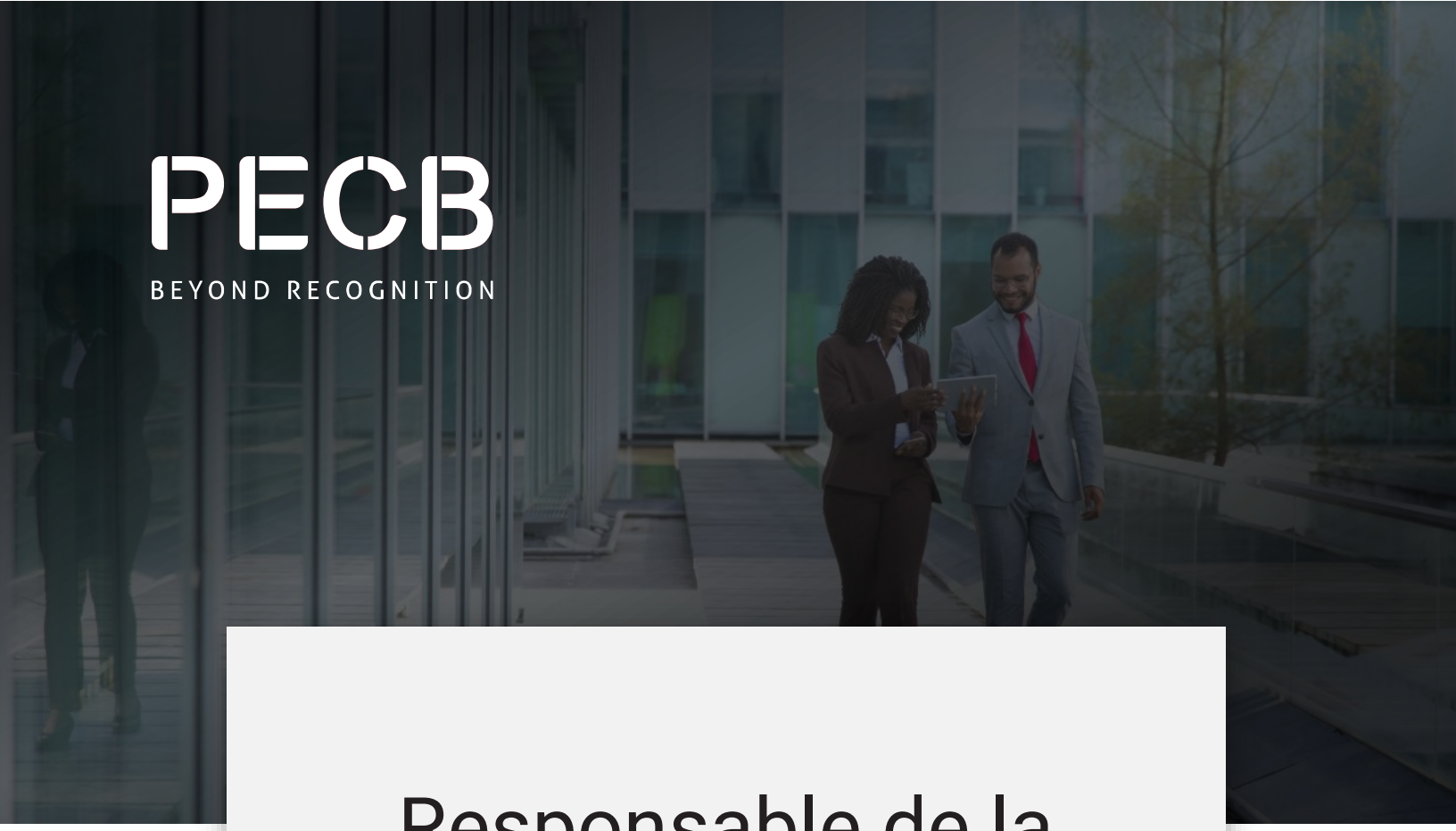

PECB

BEYOND RECOGNITION

Responsable de la sécurité du système d'information (RSSI)

Manuel du candidat

PECB

Table des matières

PECB

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui offre des programmes de formation[1] et des certifications de personnes dans un large éventail de disciplines.

Grâce à notre présence dans plus de 150 pays, nous aidons les professionnels à démontrer leur compétence dans divers domaines d'expertise en fournissant de précieux programmes d'évaluation, de certificats et de certifications selon des normes internationalement reconnues.

Nos principaux objectifs sont les suivants :

1. Établir les exigences minimales nécessaires à la certification des professionnels et à l'octroi des désignations.
2. Effectuer la revue et la vérification des qualifications des personnes afin de s'assurer qu'ils sont éligibles à la certification.
3. Maintenir et améliorer en permanence le processus d'évaluation pour la certification des personnes.
4. Certifier les personnes qualifiées, attribuer les certifications et tenir à jour les répertoires correspondants.
5. Établir des exigences pour le renouvellement périodique des certifications et s'assurer que les personnes certifiées se conforment à ces exigences.
6. S'assurer que les professionnels de PECB satisfont aux normes éthiques dans leur pratique professionnelle.
7. Représenter nos parties prenantes dans les questions d'intérêt commun.
8. Faire connaitre les avantages de la certification et des programmes de certification aux professionnels, des entreprises, des gouvernements et du public.

Notre mission

Fournir à nos clients des services complets d'examen, de certification et de programme de délivrance de certifications qui inspirent la confiance et profitent à la société dans son ensemble.

Notre vision

Se positionner comme la référence mondiale en matière de services de certification professionnelle et de programmes de certification.

Nos valeurs

Intégrité, professionnalisme, impartialité

[1] Le terme éducation renvoie aux formations développées par PECB et offertes dans le monde entier par nos partenaires.

PECB

Valeur de la certification PECB

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

La valeur des certifications de PECB est reconnue par l'accréditation de l'International Accreditation Service (IAS-PCB-111), la reconnaissance du service d'accréditation du Royaume-Uni (UKAS-No.21923) et celle de l'Office coréen d'accréditation (KAB-PC-08) conformément à la norme ISO/IEC 17024 - Exigences générales pour les organismes procédant à la certification de personnes. La valeur des programmes de certification de PECB est reconnue par l'accréditation de l'ANSI National Accreditation Board (ANAB-Accreditation ID 1003) conformément à la norme ANSI/ASTM E2659-18, Standard Practice for Certificate Programs (Pratique standard pour les programmes de certification).

PECB est membre associé du The 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 (LPP) par le Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) pour la norme Cybersecurity Maturity Model Certification (CMMC). PECB est également agréé par le Club EBIOS pour la certification EBIOS Risk Manager Skills et est agréé par la CNIL (Commission Nationale de l'Informatique et des Libertés) pour la certification DPO. Pour plus d'informations, cliquez ici.

Des 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 bonnes pratiques et méthodologies.

Conformité aux normes
Nos certifications et nos programmes de certification attestent de la conformité aux normes ISO/IEC 17024 et ASTM E2659. Ils veillent à ce que les exigences des normes soient respectées et validées avec la cohérence, le professionnalisme et l'impartialité qui s'imposent.

Un service client orienté vers la satisfaction de la clientèle
Nous sommes une entreprise orientée client et nous traitons tous nos clients avec considération, respect, professionnalisme et honnêteté. PECB dispose d'une équipe d'experts chargés de répondre aux demandes, aux questions et aux besoins. Nous faisons de notre mieux pour maintenir un temps de réponse maximum de 24 heures sans compromettre la qualité du service.

Flexibilité et confort
Les sessions de formation en ligne rendent votre parcours professionnel plus pratique, car vous pouvez programmer vos sessions de formation 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.

PECB

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. Par ailleurs, la division 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 avec les parties prenantes internes et externes, telles que les demandeurs, les candidats, les personnes certifiées, les titulaires de certificats, les autorités d'accréditation et les autorités gouvernementales.

PECB est convaincu que pour réussir, tout organisme doit acquérir une parfaite connaissance des besoins et des attentes de ses clients et des parties prenantes. Pour ce faire, PECB encourage 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 notre 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 d'améliorer continuellement leurs compétences et leurs connaissances
4. Fournir exclusivement des services pour lesquels ils sont qualifiés et compétents et informer de manière adéquate les clients et les consommateurs de la nature des services proposés, y compris de toute préoccupation ou de tout risque pertinent
5. Informer leur employeur ou leurs clients de tout intérêt ou affiliation professionnelle susceptible d'influencer ou d'altérer son jugement
6. Préserver la confidentialité des informations relatives à tout employeur ou client, actuel ou ancien, au cours de 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. Éviter de communiquer des informations intentionnellement fausses ou falsifiées susceptibles de compromettre l'intégrité du processus d'évaluation d'un candidat à une certification PECB ou à un programme de certificat PECB
10. Éviter de se présenter à tort ou à travers comme des représentants de PECB sans licence appropriée ou d'utiliser à mauvais escient le logo, les certifications ou les certificats de PECB

11. Éviter d'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 infraction présumée au présent code de déontologie

Vous pouvez consulter la version complète du code d'éthique de PECB sur la page Code d'éthique de PECB.

Introduction au rôle du RSSI (responsable de la sécurité du système d'information)

Avec l'évolution du paysage numérique, la sécurité des biens des organismes et de l'infrastructure d'information est devenue cruciale. Par conséquent, le rôle du RSSI n'a jamais été aussi crucial. Les organismes du monde entier sont confrontés à de nombreuses menaces pour la sécurité de l'information, et il incombe au RSSI de naviguer dans ces environnements complexes, en veillant à la fois à la sécurité et à la conformité. Cette formation permettra aux participants d'acquérir une compréhension globale des stratégies, des technologies et des compétences de leadership essentielles au rôle du RSSI.

Cette formation englobe les dernières méthodologies d'appréciation des risques, les cadres de gouvernance, les stratégies de réponse aux incidents et l'ensemble des menaces émergentes. Il détaille le rôle du RSSI dans la gestion de la sécurité, la prise de mesures proactives, la création de stratégies dynamiques et la promotion d'une culture organisationnelle sensibilisée à la sécurité. Au terme de cette formation, les participants seront en mesure de mettre en œuvre un programme holistique de sécurité de l'information et d'assurer la conformité avec les cadres et réglementations en matière de sécurité.

La certification « Chief Information Security Officer » atteste des compétences d'un individu dans la mise en place et la conduite d'un programme de sécurité de l'information. Grâce à cette certification, les titulaires améliorent leurs compétences pour relever les défis contemporains en matière de sécurité de l'information et se positionner en tant que leaders dans ce domaine.

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

Le présent document décrit le schéma de certification PECB Chief Information Security Officer, conformément à la norme ISO/IEC 17024:2012. Il décrit également les mesures que les candidats doivent prendre pour obtenir et conserver leurs titres. Il est donc très important de lire attentivement toutes les informations contenues dans ce document avant de remplir et d'envoyer votre demande. Pour toute question ou complément d'information, veuillez contacter le bureau international de PECB à l'adresse suivante : certification.team@pecb.com.

SECTION II : POLITIQUES ET RÈGLEMENTS RELATIFS À LA PRÉPARATION AUX EXAMENS

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 suivre la formation pour pouvoir se présenter à l'examen, le faire peut augmenter de manière significative leurs chances de réussir l'examen.

Deux options s'offrent aux candidats pour planifier l'examen :

1. Contactez l'un de nos partenaires agréés. Pour trouver un partenaire agréé 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. Vous pouvez passer un examen PECB à distance grâce à l'application PECB Exams. Pour planifier un examen en ligne, 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 passer 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 ayant suivi la formation auprès d'un des partenaires PECB, les frais d'inscription couvrent les coûts de l'examen (première tentative et première reprise), la demande de certification et la première année de frais de maintenance annuelle (FAM).

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

PECB

Domaines de compétence

Le titre RSSI est une certification professionnelle destinée aux personnes souhaitant faire valoir leur expertise dans la mise en œuvre et la direction d'un programme complet de sécurité de l'information.

Le rôle de RSSI englobe un large éventail de responsabilités et nécessite donc un ensemble de compétences variées. Si les connaissances et l'expertise techniques sont essentielles, la compétence la plus importante pour qu'un RSSI puisse diriger efficacement un programme de sécurité de l'information est sans doute le leadership stratégique.

La certification RSSI s'adresse aux :

- Professionnels qui participent activement à la gestion de la sécurité de l'information.
- Les RSSI expérimentés désireux d'approfondir leurs connaissances, de se tenir au courant des dernières tendances et d'affiner leurs compétences en matière de leadership.
- Responsables informatiques chargés de superviser les programmes et les biens liés à la sécurité de l'information.
- Professionnels de la sécurité qui aspirent à accéder à des postes de direction, tels que les architectes ou les analystes de la sécurité.
- Professionnels responsables de la gestion des risques et de la conformité en matière de sécurité de l'information au sein des organismes
- Cadres, y compris les DSI, les PDG et les directeurs de l'exploitation, qui jouent un rôle crucial dans les processus de prise de décision liés à la sécurité de l'information
- Professionnels qui souhaitent occuper des postes de direction dans le domaine de la sécurité de l'information.

Le contenu de l'examen est réparti comme suit :

- **Domaine 1 :** Concepts fondamentaux de la sécurité de l'information
- **Domaine 2 :** Rôle du RSSI dans un programme de sécurité de l'information
- **Domaine 3 :** Sélection d'un programme de conformité en matière de sécurité, gestion des risques, architecture et conception de la sécurité
- **Domaine 4 :** Aspects opérationnels des mesures de sécurité de l'information, de la gestion des incidents et de la gestion des changements
- **Domaine 5 :** Promotion d'une culture de la sécurité de l'information, contrôle, mesure et amélioration d'un programme de sécurité de l'information

PECB

Domaine 1 : Concepts fondamentaux de la sécurité de l'information

Objectif principal : S'assurer que le candidat est capable de comprendre les concepts et principes fondamentaux de la sécurité de l'information.

Compétences	Énoncés de connaissances
1. Capacité à expliquer les principaux concepts de la sécurité de l'information. 2. Capacité à expliquer les notions de confidentialité, d'intégrité et de disponibilité (la triade CIA) 3. Capacité à expliquer la divulgation, l'altération et le déni (la triade DAD) 4. Capacité à expliquer le cadre de sécurité de l'identification, de l'authentification, de l'autorisation et de la responsabilité (IAAA) 5. Capacité à identifier et à classer les différents types de menaces et de vulnérabilités 6. Capacité à reconnaître et à atténuer les attaques courantes des fournisseurs 7. Capacité à expliquer les politiques et procédures de sécurité de l'information 8. Capacité à classifier les mesures de sécurité 9. Capacité à identifier les types de logiciels malveillants et les attaques d'ingénierie sociale 10. Capacité à percevoir l'importance de la sécurité physique, de la sécurité des réseaux, de la sécurité des applications, de la sécurité cloud, de la veille sur les menaces et de la cryptographie dans la protection des biens informationnels	1. Connaissance des principaux concepts et principes de la sécurité de l'information 2. Connaissance de la triade CIA 3. Connaissance de la triade DAD 4. Connaissance du cadre de sécurité de l'identification, de l'authentification, de l'autorisation et de la responsabilité (IAAA) 5. Connaissance des différents types de menaces et de vulnérabilités 6. Connaissance des politiques et des procédures de sécurité 7. Connaissance des risques liés à la sécurité de l'information 8. Connaissance du type et de la fonction des mesures de sécurité 9. Connaissance des différentes normes et cadres de sécurité 10. Connaissance des logiciels malveillants et des attaques d'ingénierie sociale 11. Connaissance des notions de sécurité physique, de sécurité des réseaux, de sécurité des applications, de renseignement sur les menaces et de cryptographie

PECB

Domaine 2 : Rôle du RSSI dans un programme de sécurité de l'information

Objectif principal : S'assurer que le candidat est capable de définir, d'établir, de gérer et d'améliorer un programme de sécurité de l'information, tout en incarnant avec succès le rôle d'un RSSI en alignant les impératifs de sécurité sur les objectifs de l'organisme.

Compétences	Énoncés de connaissances
1. Capacité à définir le rôle et les responsabilités d'un RSSI au sein d'un organisme. 2. Capacité à collaborer et à coopérer avec d'autres cadres supérieurs 3. Capacité à comprendre et à comparer les responsabilités du RSSI, du DSI, du DGI et du RC 4. Capacité à aborder et à surmonter les défis courants rencontrés par un RSSI. 5. Capacité à développer les aptitudes au leadership nécessaires au rôle du RSSI 6. Capacité à respecter les normes éthiques 7. Capacité à définir des objectifs clairs et pertinents en matière de sécurité de l'information, alignés sur les objectifs de l'organisme 8. Capacité à mettre en place un programme complet de sécurité de l'information 9. Capacité à concevoir et à mettre en œuvre une structure organisationnelle efficace pour le programme de sécurité de l'information 10. Capacité à définir la portée d'un programme de sécurité de l'information 11. Capacité à allouer et à gérer efficacement les ressources du programme de sécurité de l'information 12. Capacité à élaborer et à mettre en œuvre des stratégies proactives en matière de sécurité de l'information	1. Connaissance des principales responsabilités d'un RSSI au sein d'un organisme. 2. Connaissance des responsabilités du RSSI, du DSI, du DGI et du RC 3. Connaissance des principales aptitudes au leadership nécessaires à la fonction de RSSI 4. Connaissance des stratégies de communication efficaces 5. Connaissance des défis potentiels auxquels un RSSI peut être confronté 6. Connaissance des considérations et des normes éthiques relatives au rôle de RSSI 7. Connaissance du programme de sécurité de l'information 8. Connaissance des objectifs en matière de sécurité de l'information 9. Connaissance des structures organisationnelles qui sous-tendent la sécurité de l'information 10. Connaissance du périmètre d'un programme d'information 11. Connaissance des ressources, des outils et du personnel indispensables à la mise en place d'un programme de sécurité de l'information efficace. 12. Connaissance de la planification et de la mise en œuvre stratégique dans le contexte de la sécurité de l'information

PECB

Domaine 3 : Sélection d'un programme de conformité en matière de sécurité, gestion des risques, architecture et conception de la sécurité

Objectif principal : S'assurer que le candidat est capable d'interpréter, de développer et de maintenir le programme de conformité d'un organisme, de gérer efficacement les risques, d'analyser les mesures de sécurité existantes et de concevoir des architectures de sécurité robustes en choisissant une architecture de sécurité et un cadre de conception approprié.

Compétences	Énoncés de connaissances
1. Capacité à élaborer, mettre en œuvre et contrôler un programme de conformité en fonction des besoins spécifiques de l'organisme	1. Connaissance des principaux cadres réglementaires et des normes applicables au secteur
2. Capacité à garantir le respect des réglementations et des normes spécifiques à un secteur d'activité	2. Connaissance des différents organismes et de leur rôle spécifique en matière de sécurité de l'information
3. Capacité à revoir et à mettre à jour régulièrement le programme de conformité.	3. Connaissance des fonctions essentielles, des catégories et des sous-catégories décrites dans le cadre de cybersécurité du NIST
4. Capacité à sensibiliser et à former les employés aux exigences de conformité et aux bonnes pratiques	4. Connaissance des niveaux de mise en œuvre et de la manière dont ils soutiennent le processus de gestion des risques
5. Capacité à assurer la coordination avec les services juridiques et les autres services afin de garantir une conformité totale	5. Connaissance des objectifs et des exigences de la directive NIS 2
6. Capacité à identifier, évaluer et classer les risques par ordre de priorité dans le contexte de l'organisme	6. Connaissance des méthodes de mise en œuvre et de suivi de l'efficacité des mesures de sécurité du CIS
7. Capacité à évaluer l'efficacité des mesures de sécurité	7. Connaissance de la structure du cadre COBIT, y compris ses composantes de gouvernance et ses pratiques de gestion
8. Capacité à identifier les failles dans les mesures de sécurité existantes	8. Connaissance des exigences de la norme ISO/IEC 27001 relative à un système de gestion de la sécurité de l'information (SGSI)
9. Capacité à examiner les capacités de sécurité de l'information dans des domaines clés tels que le risque et la résilience, le renseignement et la sensibilisation, la sécurité opérationnelle, la sécurité physique et la gestion de la chaîne d'approvisionnement	9. Connaissance des cinq étapes ITIL, des exigences PCI DSS, du programme CSA STAR, du RGPD et de l'HIPPA
10. Capacité à utiliser l'analyse des failles dans l'identification et l'évaluation des capacités existantes en matière de sécurité de l'information	10. Connaissance de la politique de sécurité de l'information et de son rôle dans l'orientation du comportement de l'organisme et dans la garantie de la conformité à la sécurité
11. Capacité à élaborer et à mettre en œuvre des stratégies d'atténuation des risques	11. Connaissance des capacités en matière de sécurité de l'information
12. Capacité à identifier, analyser et évaluer les risques	12. Connaissance des capacités de gestion de la chaîne d'approvisionnement
	13. Connaissance des méthodes d'appréciation des risques

13. Capacité à sélectionner les options de traitement des risques liés à l'information 14. Capacité à élaborer un plan de traitement des risques 15. Capacité à identifier les outils et les logiciels de gestion des risques qui peuvent être utilisés pour automatiser les processus 16. Capacité à faire le lien entre la communication sur les risques et les objectifs de l'entreprise 17. Capacité à établir un plan de communication sur les risques avec les parties internes et externes 18. Capacité d'enregistrer, de signaler, de surveiller et d'examiner les risques 19. Capacité à expliquer l'architecture et la conception de la sécurité 20. Capacité à sélectionner un cadre d'architecture, de sécurité et à l'aligner sur les ressources de l'entreprise 21. Capacité à expliquer le principe de l'architecture « Zero trust » 22. Capacité à sélectionner les éléments de conception de l'architecture de sécurité 23. Capacité à expliquer la différence entre les systèmes de sécurité de l'information et la sécurité des infrastructures	14. Connaissance des techniques et des outils d'atténuation des risques 15. Connaissance des principes de la surveillance continue de la gestion des risques 16. Connaissance des techniques d'identification des risques, des méthodes d'analyse des risques et des critères d'évaluation des risques 17. Connaissance du processus de traitement des risques (traitement, atténuation, transfert ou acceptation des risques) 18. Connaissance des stratégies de communication efficaces en matière de risques 19. Connaissance des mécanismes de surveillance et de revue permettant d'améliorer le processus de gestion des risques 20. Connaissance des cadres et des méthodologies qui guident une gestion efficace des risques 21. Connaissance des principes et des structures des architectures de sécurité organisationnelles et de leur application 22. Connaissance des cadres d'architecture de sécurité Zachman, SABSA, TOGAF et OSA 23. Connaissance du principe du « Zero trust » 24. Connaissance des composants de l'architecture de sécurité tels que NFV, SASE, SSE, services de réseaux superposés et architecture multicloud

PECB

Domaine 4 : Aspects opérationnels des mesures de sécurité de l'information, de la gestion des incidents et de la gestion des changements

Objectif principal : S'assurer que le candidat est capable de sélectionner, concevoir, mettre en œuvre et évaluer les mesures de sécurité de l'information, de gérer les incidents de sécurité et de superviser le processus de gestion des changements informatiques.

Compétences	Énoncés de connaissances
1. Capacité à classer, sélectionner et mettre en œuvre des mesures efficaces de sécurité de l'information	1. Connaissance des différentes classifications des mesures de sécurité de l'information
2. Capacité à documenter de manière exhaustive les mesures de sécurité de l'information mises en place	2. Connaissance des processus et des bonnes pratiques en matière de sélection et de conception des mesures de contrôle
3. Capacité à mettre en œuvre des mesures spécifiques pour le renseignement sur les menaces et la sécurité opérationnelle	3. Connaissance des normes de documentation pour les mesures de sécurité de l'information
4. Capacité à intégrer la sécurité physique dans le cadre plus large des mesures de sécurité de l'information	4. Connaissance des mesures spécifiques au renseignement sur les menaces et de leurs applications
5. Capacité à concevoir et à mettre en œuvre des mesures de contrôle pour la gestion de la chaîne d'approvisionnement	5. Connaissance des éléments clés des mesures de sécurité opérationnelles et physiques
6. Capacité à identifier les technologies émergentes pertinentes pour les RSSI	6. Connaissance des mesures de gestion de la chaîne d'approvisionnement et de leur importance pour assurer un chiffrement de bout en bout
7. Capacité à tester et à évaluer l'efficacité des mesures de sécurité établies	7. Connaissance des technologies émergentes et de leurs implications pour les RSSI
8. Capacité à gérer efficacement les incidents liés à la sécurité de l'information	8. Connaissance des protocoles de test et des mesures d'évaluation des mesures de sécurité
9. Capacité à surveiller, documenter et signaler les incidents de sécurité	9. Connaissance du cycle de vie de la gestion des incidents de sécurité de l'information
10. Capacité à concevoir et à mettre en œuvre des programmes de formation à la réponse aux incidents et de sensibilisation à la sécurité	10. Connaissance des techniques de surveillance et des normes de documentation des incidents de sécurité
11. Capacité à élaborer des plans de continuité d'activité	11. Connaissance de la conception de modules de formation à la réponse aux incidents et de l'importance des programmes de sensibilisation à la sécurité
12. Capacité à élaborer et à mettre en œuvre un plan de reprise après sinistre	12. Connaissance de la planification de la continuité d'activité
13. Capacité à expliquer et à mettre en œuvre les processus de gestion des changements informatiques	13. Connaissance de la planification de la reprise après sinistre
14. Capacité à catégoriser et à classer par ordre de priorité les changements informatiques en fonction de leur impact et de leur pertinence	14. Connaissance de la gestion des changements informatiques et de son importance
	15. Connaissance des trois catégories de changements informatiques

15. Capacité à mettre en place des mesures de gestion des changements afin de superviser et d'assurer la réussite des transitions 16. Capacité à reconnaître et à assumer les rôles et les responsabilités dans la gestion des changements informatiques, y compris le rôle du RSSI	16. Connaissance des mécanismes de contrôle de la gestion des changements 17. Connaissance de la procédure étape par étape pour une gestion efficace des changements informatiques 18. Connaissance des différents rôles et responsabilités au sein de la gestion des changements informatiques 19. Connaissance du rôle du RSSI dans la supervision et l'orientation de la gestion des changements informatiques

PECB

Domaine 5 : Promotion d'une culture de la sécurité de l'information, contrôle, mesure et amélioration d'un programme de sécurité de l'information

Objectif principal : S'assurer que le candidat est capable d'élaborer et d'évaluer des programmes de formation et de sensibilisation efficaces, de mettre en place un processus de contrôle solide et de comprendre l'importance des programmes d'assurance.

Compétences	Énoncés de connaissances
1. Capacité à établir et à améliorer un programme de formation et de sensibilisation	1. Connaissance des éléments clés des programmes de sensibilisation et de formation
2. Capacité à assumer les responsabilités du RSSI dans le cadre du programme de sensibilisation et de formation	2. Connaissance du rôle du RSSI dans l'orientation et la direction des activités de formation et de sensibilisation
3. Capacité à allouer efficacement des fonds au programme de formation et de sensibilisation	3. Connaissance des besoins de financement et des stratégies d'attribution des programmes de formation
4. Capacité à concevoir des structures de programmes de développement des compétences	4. Connaissance des différents structures et types de programmes de développement des compétences
5. Capacité à sélectionner et à mettre en œuvre des méthodes de formation efficaces	5. Connaissance des différentes méthodes de formation et de leur efficacité
6. Capacité à s'adapter et à expliquer les changements culturels au sein de l'organisme	6. Connaissance des mécanismes de changement culturel au sein des organismes
7. Capacité à évaluer les résultats des sessions de formation	7. Connaissance des techniques d'évaluation des résultats de la formation
8. Capacité à mettre en œuvre des pratiques de surveillance continue de la sécurité de l'information	8. Connaissance du contrôle continu de la sécurité de l'information (ISCM) et de son importance
9. Capacité à apprécier l'efficacité globale du programme de sécurité de l'information	9. Connaissance des techniques d'appréciation pour l'évaluation du programme de sécurité
10. Capacité à définir et à utiliser des mesures de sécurité pertinentes et des indicateurs clés de performance (ICP)	10. Connaissance de la conception de mesures et d'indicateurs clés de performance pertinents pour la sécurité de l'information
11. Capacité à évaluer les performances et à revoir les indicateurs clés de performance	11. Connaissance de l'évaluation des performances et des indicateurs de performance clé
12. Capacité à communiquer efficacement les résultats des mesures	12. Connaissance des mécanismes efficaces de communication des résultats de l'évaluation
13. Capacité à expliquer et à mettre en œuvre un programme d'assurance	13. Connaissance des fondements et de l'importance d'un programme d'assurance
14. Capacité à tester, examiner et rendre compte des procédures de sécurité de l'information	14. Connaissance des techniques permettant de tester et d'examiner les procédures de sécurité de l'information et de rendre compte des résultats
15. Capacité à mener des audits de sécurité complets	
16. Capacité à expliquer l'importance des tests d'intrusion et à en analyser les résultats	

17. Capacité à intégrer les activités d'analyse de la vulnérabilité dans le programme d'assurance de l'organisme 18. Capacité à apprécier la situation générale de l'organisme en matière de sécurité 19. Capacité à guider et à superviser les audits internes et externes	15. Connaissance des procédures d'audit de sécurité 16. Connaissance des méthodes d'appréciation des risques et de leur impact sur la sécurité 17. Connaissance des principes et pratiques des tests d'intrusion 18. Connaissance des outils et méthodologies d'analyse de la vulnérabilité 19. Connaissance des appréciations de la démarche de sécurité 20. Connaissance des processus d'audit interne et externe

Sur la base des domaines susmentionnés et de leur pertinence, l'examen contient 80 questions à choix multiples, comme le résume le tableau ci-dessous :

				Niveau de compréhension (cognitif/taxonomie) 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 permettant de mesurer l'évaluation
Domaines de compétence	Concepts fondamentaux de la sécurité de l'information	9	11,25	X	
	Rôle du RSSI dans un programme de sécurité de l'information	20	25	X	
	Sélection d'un programme de conformité en matière de sécurité, gestion des risques, architecture et conception de la sécurité	20	25	X	
	Aspects opérationnels des mesures de sécurité de l'information, de la gestion des incidents et de la gestion des changements	21	26,25		X
	Promotion d'une culture de la sécurité de l'information, contrôle, mesure et amélioration d'un programme de sécurité de l'information	10	12,5		X
	Total des points	**80**	**100 %**		
	Nombre de questions par niveau de compréhension			**49**	**31**
	Pourcentage de l'examen consacré à chaque niveau de compréhension (cognitif/taxonomie)			**61,25 %**	**38,75 %**

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

Lorsque les candidats réussissent l'examen, ils peuvent demander à obtenir le titre de « PECB Chief Information Security Officer ».

PECB

Passer l’examen

Informations générales au sujet de l’examen
Les candidats sont tenus d'être présents au moins 30 minutes avant le début de l'examen.

Les candidats qui arrivent en retard ne disposeront pas de temps supplémentaire pour compenser leur retard et pourraient se voir refuser l'accès à l'examen.

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

Si la demande en est faite le jour de l'examen, un délai supplémentaire peut être accordé aux candidats qui passent l'examen dans une langue autre que leur langue maternelle.
- 10 minutes supplémentaires pour les examens Foundation
- 20 minutes supplémentaires pour les examens Manager
- 30 minutes supplémentaires pour les examens Lead

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

Pour des informations plus détaillées sur 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 multiples peut être utilisé pour évaluer la compréhension des candidats sur des concepts simples ou complexes. Il comprend à la fois des questions autonomes et des questions basées sur des scénarios. Les questions autonomes sont indépendantes de l’examen et ne dépendent pas du contexte, 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. Pour répondre aux questions autonomes et aux questions basées sur des scénarios, les candidats devront faire appel à divers concepts et principes expliqués au cours de la formation, analyser des problèmes, identifier et évaluer des alternatives, combiner plusieurs concepts ou idées, etc.

Chaque question à choix multiple comporte trois options, dont l’une est la réponse correcte (réponse codée) et les deux autres sont des réponses incorrectes (questions pour distraire).

Cet examen est à livre ouvert. Le candidat est autorisé à utiliser les documents de référence suivants :

- Supports de formation du participant (accessibles via l'application PECB Exams ou imprimés)
- Notes personnelles prises pendant la session de formation (accessibles via l'application PECB Exams ou imprimés)
- Dictionnaire au format papier

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

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

Pour des informations spécifiques sur les types d'examens, les langues disponibles et d'autres détails, veuillez contacterexamination.team@pecb.com consulter la Liste des examens PECB.

PECB

Exemples de questions d'examen

Zootron, une entreprise allemande leader dans le secteur de la technologie, a récemment procédé à une transformation structurelle de son département informatique. Consciente de la recrudescence des cybermenaces, l'entreprise a créé un poste dédié, celui de RSSI. Jenah, qui possède une expérience à la fois dans le domaine de la technologie et de la gestion, a été nommée à ce poste.

Au cours du premier mois, Jenah a passé en revue les principes fondamentaux de la sécurité de l'information. Elle a constaté des failles dans la gestion des risques de cybersécurité et la non-conformité aux normes de confidentialité et de sécurité. Elle a également identifié les risques par le biais d'une appréciation détaillée.

Dès le troisième mois, Jenah a lancé un programme de sensibilisation et de formation. Elle a plaidé en faveur d'une culture de travail positive, a stimulé la productivité et a obtenu des financements pour la formation, en veillant à ce qu'un ensemble de méthodes combinées permette de répondre aux besoins de tous les apprenants. Elle a également souligné la nécessité d'une surveillance continue et de la mise en œuvre de pratiques de gestion des risques, de suivi des anomalies, d'évaluation des vulnérabilités et d'identification des menaces. Elle a utilisé des outils fournissant des indications sur diverses mesures de sécurité afin d'évaluer l'efficacité du programme de sécurité de l'information de *Zootron*.

Au bout de six mois, Jenah a proposé de lancer un programme d'assurance. Il s'agissait notamment d'un audit de sécurité approfondi visant à évaluer le réseau de l'entreprise, à identifier les faiblesses et à garantir la conformité avec les normes et réglementations applicables. Les audits ont été menés par les professionnels de *Zootron* qui ont également été chargés de conseiller l'organisme sur les mesures d'amélioration. De plus, Jenah a proposé l'utilisation d'outils pour détecter les risques potentiels de sécurité dans le système de *Zootron*, ainsi que des attaques de piratage simulées pour identifier les causes profondes des attaques de cybersécurité. Cette initiative aiderait *Zootron* à identifier les points faibles des capacités existantes de l'organisme en matière de protection des composants technologiques, des services et des applications logicielles de sécurité de l'information, ainsi que des systèmes basés sur le cloud.

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

1. **Sur la base des informations recueillies par Jenah au cours du premier mois, quels cadres de conformité l'entreprise doit-elle mettre en œuvre ?**
   A. COBIT et HIPAA
   B. **NIST CSF et RGPD**
   C. Mesures CIS et programme CSA STAR

2. **Lorsque Jenah a lancé un programme de sensibilisation et de formation, sur quoi a-t-elle mis l'accent ?**
   A. Le strict respect des protocoles de sécurité
   B. La collaboration entre les services
   C. **Le changement culturel**

3. **Comment Jenah s'est-elle assurée de l'efficacité du programme de sécurité de l'information de *Zootron* ?**
   A. **En mettant en œuvre des pratiques ISCM et des indicateurs de performance (ICP).**
   B. En se concentrant exclusivement sur les programmes de sensibilisation à la formation.
   C. En réalisant un audit externe.

4. **Sur la base du scénario ci-dessus, Jenah a proposé de simuler des attaques de piratage au sein de *Zootron* afin d'identifier les causes profondes des attaques potentielles. Est-ce acceptable ?**
   A. **Oui, des simulations d'attaques peuvent être effectuées par des utilisateurs autorisés au sein de l'organisme.**
   B. Non, les simulations d'attaques sont contraires à l'éthique et ne peuvent être menées par des personnes au sein de l'organisme.
   C. Non, Jenah aurait dû attendre que de véritables attaques se produisent pour en identifier la cause profonde

5. **Quelle capacité de sécurité de l'information de *Zootron* l'initiative du programme d'assurance de Jenah visait-elle à améliorer ?**
   A. Gestion de la chaîne d'approvisionnement
   B. **Sécurité opérationnelle**
   C. Le renseignement sur les menaces

PECB

Politique de sécurité des examens

PECB est résolu 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 et des partenaires pour maintenir la confidentialité des examens de PECB. Cette politique vise à lutter contre les comportements inacceptables et à garantir un traitement équitable de tous les candidats.

Toute divulgation d'informations sur le contenu des examens de PECB constitue une violation directe de la présente politique et du code d'éthique de PECB. Par conséquent, les candidats qui se présentent à un examen 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 contenues dans le support 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 ni 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 support relatif à l'examen.
4. Les candidats ne sont pas autorisés à copier ou à tenter de faire des copies (écrites, photocopiées ou autres) du support de l'examen, y compris, mais sans s'y limiter, des questions, des réponses ou des images d'écran.
5. Les candidats ne doivent pas participer à des activités frauduleuses liées à la passation d'examens ni en faire la promotion, telles que :
    - Regarder le support 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 dump », 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 tenu de s'y conformer, sinon, en cas d'irrégularités, les candidats impliqués seront directement signalés à PECB ou, s'ils sont témoins de telles irrégularités, ils doivent immédiatement en faire part à PECB.

Il incombe entièrement aux candidats de comprendre et de respecter les règles et politiques de l'examen de PECB, de l'accord de confidentialité et de non-divulgation et du code de déontologie. Par conséquent, en cas de violation d'une ou de plusieurs règles, les candidats ne recevront aucun remboursement. Par ailleurs, PECB est autorisé à retirer le droit de se présenter à un examen PECB ou à inviter les candidats à repasser l'examen si des irrégularités sont constatées pendant et après la procédure de notation, en fonction de la gravité de la violation.

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 support d'examen, y compris l'obtention d'une injonction immédiate.

PECB prendra des mesures à l'encontre des personnes qui enfreignent les règles et les politiques, y compris l'interdiction permanente d'obtenir des accréditations de PECB et la révocation de toutes les accréditations

antérieures. 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 entre trois et huit semaines pour les examens de type rédactionnel et entre deux et quatre semaines pour les examens à choix multiples sur papier.
- Pour les examens à choix multiples en ligne, les candidats reçoivent leurs résultats instantanément.

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

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

Les candidats qui ne sont pas satisfaits des résultats peuvent demander une réévaluation en écrivant à examination.team@pecb.com dans les 30 jours qui suivent la date de 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 en utilisant le Système de ticket de PECB. Toute plainte reçue après 30 jours ne sera pas traitée.

Politique de reprise d'examen

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

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

Note : Les candidats qui ont suivi la formation chez l'un de nos partenaires et qui ont échoué à la première tentative d'examen peuvent le reprendre gratuitement dans les 12 mois à compter de la date de réception du code promotionnel (le prix payé pour la formation comprend 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 promotionnel 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 une formation auprès d’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 DE CERTIFICATION ET EXIGENCES

Certification PECB CISO

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

Les certifications du programme PECB CISO répondent aux exigences suivantes :

Titre de compétence	Examen	Expérience professionnelle	Expérience en matière de projets de sécurité de l'information	Autres exigences
PECB Information Security Officer	Examen PECB Chief Information Security Officer	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Chief Information Security Officer		Cinq ans : Deux ans d'expérience en gestion de la sécurité de l'information	Activités de projet : total de 300 heures	

Pour être efficaces, les activités de sécurité de l'information d'un RSSI doivent respecter les meilleures stratégies de mise en œuvre, qui englobent les aspects clés suivants :

1. Développer des procédures opérationnelles et de communication en matière de sécurité
2. Identifier les objectifs et les mesures de sécurité
3. Veiller à ce que l'entreprise soit en conformité réglementaire avec les règles des organismes compétents
4. Faire respecter les bonnes pratiques en matière de sécurité de l'information
5. Diriger l'équipe de réponse aux incidents
6. Mener des investigations électroniques et des enquêtes médico-légales numériques
7. Organiser des formations de sensibilisation à la sécurité à l'intention des employés

Demande de 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 personnes qui seront contactées pour valider l'expérience professionnelle des candidats. Les candidats peuvent soumettre leur candidature en anglais, français, allemand, espagnol ou coréen. Ils peuvent choisir de payer en ligne ou d'être facturés. Pour plus d'informations, veuillez contacter certification.team@pecb.com.

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

- Enregistrez votre compte
- Vérifier 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 conditions de certification pour le titre concerné. Le candidat recevra un e-mail l'informant de l'état de sa candidature, y compris 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 de la certification, cliquez ici. Pour plus d'informations sur l'obtention du badge numérique, cliquez ici.

PECB offre une assistance en anglais et en français.

Expérience professionnelle

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

Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. 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 sécurité de l'information, ainsi que de ses antécédents professionnels actuels et antérieurs. Les références professionnelles de personnes qui sont sous la supervision du candidat ou qui sont ses proches ne sont pas valables.

Expérience de projet

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

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 entraîner une rétrogradation des compétences du candidat.

PECB

SECTION IV : POLITIQUES DE CERTIFICATION

Refus de la certification

PECB peut refuser la certification ou l'accès au programme de certification si le candidat :

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

Les candidats dont la demande de certification ou auquel l'accès au programme de certification a été refusé peuvent déposer une plainte dans le cadre de la procédure de réclamation et d'appel. Pour de plus amples informations, veuillez vous référer à la section **Politique en matière de plainte et d'appel**.

Le paiement de la demande d'accès au programme de certification ou pour la délivrance de la certification n'est pas remboursable.

Différents statuts de certification

Actif

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

Suspendue

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

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

Révoqué

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas à ses exigences. Dans ce cas, les candidats ne sont plus autorisés à se présenter comme des professionnels certifiés PECB. D'autres motifs de révocation de la certification peuvent être invoqués si le candidat :

- Enfreint le Code de déontologie de PECB
- Fait une fausse déclaration et fournit de fausses informations sur l'étendue 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 plainte dans le cadre de la procédure de réclamation et de recours. Pour de plus amples informations, veuillez vous référer 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, consultez la page Options de statut de certification.

Mise à niveau et rétrogradation des informations d'identification

Mise à niveau des certifications
Les professionnels peuvent améliorer leurs qualifications dès qu'ils peuvent démontrer qu'ils remplissent les conditions requises.

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

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

Note : *Les professionnels certifiés par PECB qui détiennent des certifications Lead et qui ne fournissent pas de preuves des exigences de maintien de la certification verront leurs titres déclassés. Les titulaires d'une certification Master qui ne soumettent pas de FPC et ne paient pas de FAM verront leur certification révoquée.*

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 satisfaire aux exigences liées au titre désigné, par exemple, ils doivent effectuer le nombre requis d'heures de formation professionnelle continue (FPC). Ils doivent en outre s'acquitter des frais annuels de maintien (120 $). Pour plus d'informations, consultez 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 d'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 à certification.team@pecb.com et payer les frais requis.

Politique en matière de plaintes et de recours

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

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

PECB

SECTION V : POLITIQUES GÉNÉRALES

Examens et certifications d'autres organismes de certification accrédités

PECB accepte les certifications et les examens d'autres organismes de certification accrédités et reconnus. PECB évaluera les demandes par le biais de son processus d'équivalence pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective.

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

Politique comportementale

PECB a pour objectif de 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). Ces services visent aussi 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 consulter la politique comportementale, cliquez ici.

Politique de remboursement

Si vous remplissez les conditions de la Politique de remboursement, PECB vous remboursera votre paiement. Pour consulter la Politique de remboursement, cliquez ici.

---

[3] Selon la loi américaine en faveur des personnes handicapées (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

Tel./Fax :

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

E-mails

Examen :
examination.team@pecb.com

Certification :
certification.team@pecb.com

Le 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