Catalogue de formations 2026

PECB

Dr. Eric Lachapelle
Président du conseil d'administration de PECB

Chez PECB, notre objectif est de préparer les professionnels aux défis de demain. Grâce à des formations et des certifications de haute qualité, nous fournissons aux individus les outils dont ils ont besoin pour protéger les données et la vie privée, et instaurer la confiance dans un monde axé sur le numérique. Nous mettons l'accent sur des connaissances et des compétences pratiques qui s'appliquent directement au milieu professionnel, en veillant à ce que les professionnels puissent non seulement atteindre leurs objectifs, mais aussi les dépasser. L'innovation et la croissance continue sont au cœur de tout ce que nous faisons, et c'est ainsi que nous aidons les personnes à réussir dans un environnement en constante évolution.

Dr. Faton Aliu
Président de PECB

Pour nous, l'excellence est le point de rencontre entre le savoir, l'innovation et la confiance numérique. Il s'agit de bien plus que de principes directeurs ; ils constituent le fondement du progrès dans un monde qui exige fiabilité et résilience. Alors que la sécurité et la confiance deviennent essentielles pour chaque organisation, PECB est là pour doter les professionnels et les équipes des compétences et de la confiance nécessaires pour garder une longueur d'avance.

Notre objectif est simple : aider les personnes à évoluer. Nous souhaitons que chaque apprenant, chaque partenaire et chaque organisation que nous accompagnons se sentent autonomes, équipés des bons outils, de perspectives claires et d'un état d'esprit tourné vers l'avenir. Avec PECB, la formation ne consiste pas seulement à obtenir des titres ; il s'agit d'une véritable transformation et de démarches concrètes vers des carrières plus solides et des organisations plus fortes.

TABLE DES MATIÈRES

Catalogue de formations PECB 2026

Un catalogue de formations est une collection structurée de programmes d'apprentissage qui aide les professionnels à sélectionner les formations adaptées à leurs objectifs de carrière.

Pourquoi est-ce important ?

Un catalogue de formations est essentiel, car il :

- Fournit de la **clarté** en organisant diverses options d'apprentissage en un seul endroit.
- Garantit la **pertinence** grâce à des connaissances à jour et à des certifications reconnues.
- Renforce la **confiance numérique** en dotant les professionnels de compétences qui favorisent la sécurité, la résilience et une croissance durable.

À propos de PECB

PECB est un organisme de certification mondial et un partenaire de confiance en matière de formation professionnelle.

Nous permettons aux individus et aux organisations de renforcer leur expertise, de consolider leurs compétences et de démontrer leur crédibilité dans le domaine de la sécurité numérique et au-delà.

Nos principes

Agilité
S'adapter rapidement stimule l'innovation.

Inclusivité
La diversité favorise la valeur et la connexion.

Durabilité
Des pratiques responsables garantissent un succès à long terme.

Le portefeuille diversifié de formations PECB.

PECB propose un large éventail de formations réparties en plusieurs portefeuilles. Ces formations sont conçues pour aider les professionnels à acquérir des compétences et des connaissances dans des domaines spécifiques, en leur offrant une compréhension approfondie des normes et des cadres pertinents. Les méthodes pédagogiques de PECB rendent les participants capables de mettre en œuvre et de gérer efficacement ces pratiques au sein de leurs organisations, en renforçant leur expertise dans leurs domaines respectifs.

Découvrez un aperçu des formations proposées dans chaque portefeuille désigné :

Cybersécurité

Les formations de ce portefeuille se concentrent sur la protection des systèmes d'information, l'identification et l'atténuation des cybermenaces, ainsi que sur l'élaboration de stratégies de sécurité robustes garantissant la protection et l'intégrité des données..

Continuité, résilience et reprise

Les formations de ce portefeuille préparent les professionnels à élaborer et à mettre en œuvre des stratégies garantissant la continuité des activités, la résilience organisationnelle et une reprise efficace face à des événements perturbateurs.

Protection de la vie privée et des données

Ce portefeuille couvre les lois et pratiques essentielles en matière de protection des données, notamment la conformité au RGPD, ainsi que les stratégies visant à protéger les informations personnelles et sensibles dans un monde de plus en plus axé sur les données.

IA et transformation numérique

Ce portefeuille se concentre sur l'intersection entre l'intelligence artificielle et l'innovation numérique. Ces formations aident les organisations à exploiter les technologies de l'IA et à relever les défis et opportunités liés à la transformation numérique.

Gouvernance, risque et conformité

Ce portefeuille met l'accent sur les cadres de gouvernance, la gestion des risques et les stratégies de conformité, en dotant les participants des compétences nécessaires pour aligner les objectifs organisationnels sur les exigences réglementaires et commerciales.

Qualité, santé, sécurité et durabilité

Ce portefeuille se concentre sur les systèmes de management de la qualité, la santé et la sécurité au travail, ainsi que sur des pratiques durables favorisant la réussite organisationnelle à long terme et la protection de l'environnement.

Parcours de développement professionnel : Niveaux et durées des formations

FORMATIONS SUR LES SYSTÈMES DE MANAGEMENT	À QUI S'ADRESSENT-ELLES	
FOUNDATION	Personnes qui souhaitent apprendre les bases de la mise en œuvre d'un système de management et de ses processus	**2 JOURS**
LEAD IMPLEMENTER	Personnes responsables de la mise en œuvre et du management d'un système de management au sein de leur organisation	**5 JOURS**
LEAD AUDITOR	Personnes responsables de l'audit et de la surveillance des systèmes de management	**5 JOURS**
FORMATIONS DE MANAGER		
FOUNDATION	Personnes qui souhaitent étudier les principes fondamentaux des processus et procédures dans le domaine ou la norme concernée	**2 JOURS**
MANAGER / OFFICER	Managers du domaine concerné qui souhaitent développer les compétences et les connaissances nécessaires pour réaliser et mettre en œuvre des processus, des approches et des techniques pour différents programmes, plans, stratégies, etc.	**3 JOURS**
LEAD MANAGER / OFFICER	Managers du domaine concerné qui souhaitent évaluer, gérer ou maintenir des plans, des évaluations, des cadres, des programmes ou des éléments similaires, et développer leur expertise en management	**5 JOURS**
FORMATIONS NON ISO		
FOUNDATION	Personnes qui souhaitent étudier les fondements du domaine associé et de ses processus connexes	**2 JOURS**
MANAGER / OFFICER	Managers du domaine concerné qui souhaitent acquérir des connaissances sur les principes et concepts fondamentaux d'un programme de management	**3 JOURS**
LEAD MANAGER / OFFICER / PROFESSIONAL AND ANALYST	Managers du domaine concerné qui souhaitent développer leurs compétences et leurs connaissances dans le domaine associé et améliorer leur expertise en management	**5 JOURS**
FORMATIONS EN CYBERSÉCURITÉ TECHNIQUE		**5 JOURS**
SÉCURITÉ OFFENSIVE	Professionnels qui souhaitent en savoir plus sur les tactiques et techniques utilisées par les pirates informatiques malveillants et améliorer leur capacité à protéger leurs systèmes	**5 JOURS**
SÉCURITÉ DÉFENSIVE	Personnes qui souhaitent améliorer de manière significative leurs capacités défensives et apprendre les bonnes pratiques pour le durcissement des systèmes et la configuration efficace de la sécurité	**5 JOURS**
INFORMATIQUE LÉGALE	Professionnels qui souhaitent acquérir un large éventail de compétences et de connaissances essentielles à l'informatique légale	**5 JOURS**

Votre certification PECB est votre crédibilité !

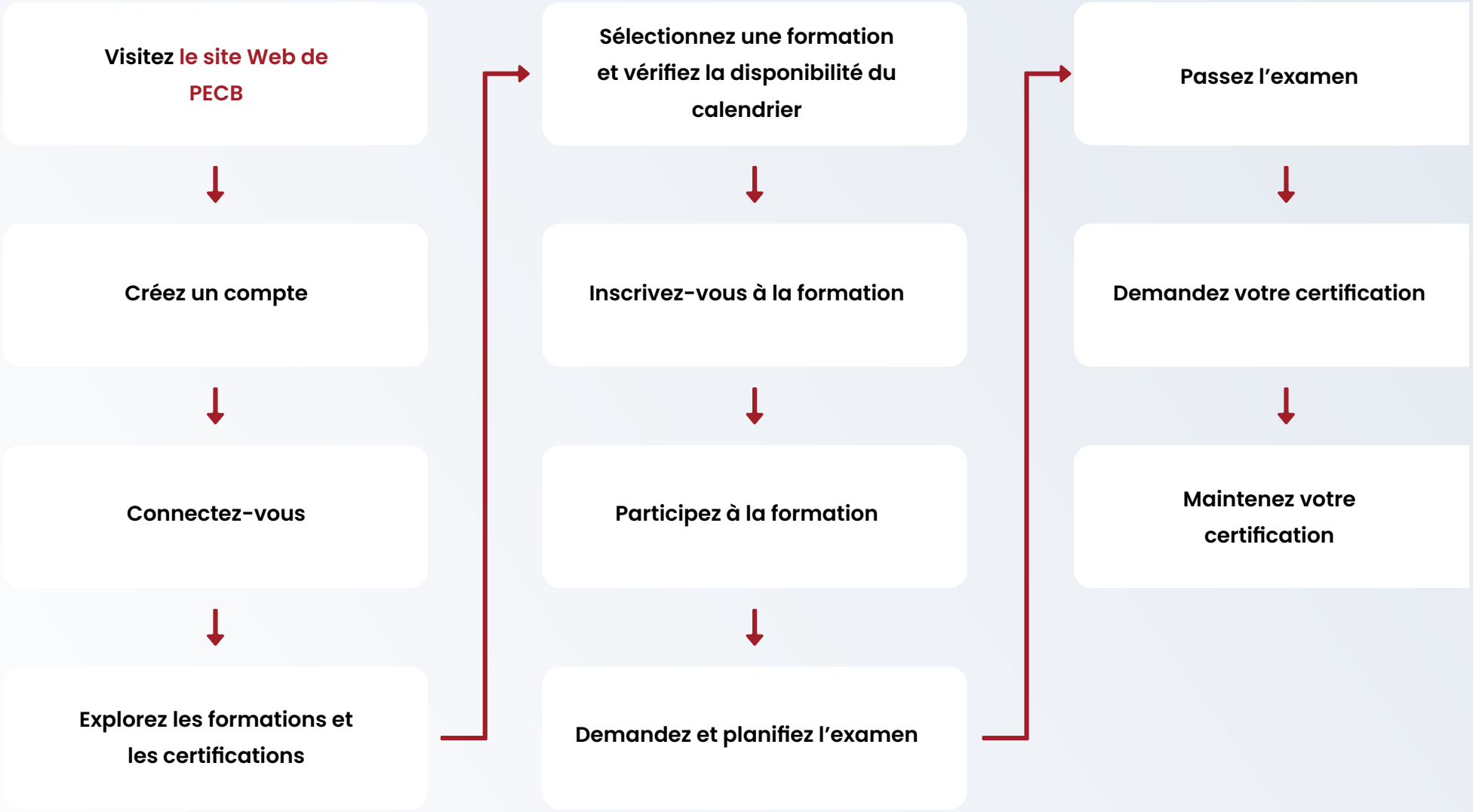
La certification professionnelle constitue une preuve officielle de formation, de compétence et de reconnaissance professionnelle. Mais au-delà de cela, les certifications délivrées par PECB démontrent que vous êtes une personne engagée et déterminée à poursuivre votre développement professionnel. Plus important encore, elles attestent que vous avez acquis des compétences et des connaissances validées.

Que vous soyez au début de votre parcours ou que vous disposiez déjà d'une carrière réussie dans le domaine des normes ISO et d'autres cadres réglementaires, la certification PECB valorise votre parcours professionnel et garantit une plus grande réussite dans la profession que vous avez choisie.

Nos certifications vous aident à exécuter vos tâches et constituent des preuves fiables que vous avez satisfait aux exigences minimales en matière de comportement professionnel et éthique, tout en vous aidant à accomplir et à gérer plus efficacement toutes vos tâches.

Un investissement qui constitue assurément un investissement rentable de votre temps et de vos ressources — car une soif continue de connaissances se traduit par une entreprise florissante et un développement professionnel durable.

Parcours du processus d'inscription, d'enregistrement et de certification



**Il est recommandé de suivre une formation PECB ou toute autre formation, mais cela n'est pas obligatoire, sauf pour les programmes de certificat Foundation accrédités par l'ANAB, pour lesquels la participation à la formation PECB correspondante est obligatoire*

Critères de certification : Désignation, expérience et exigences en matière de projets

EXAMEN	DÉSIGNATION	EXPÉRIENCE PROFESSIONNELLE	EXPÉRIENCE D'AUDIT	EXPÉRIENCE DE PROJET
FOUNDATION	Foundation	-	-	-
LEAD MANAGER	Provisional Manager	-	-	-
	Manager	2 ans (dont 1 dans le domaine spécialisé)	-	200 heures
	Lead Manager	5 ans (dont 2 dans le domaine spécialisé)	-	300 heures
	Senior Lead Manager	10 ans (dont 7 dans le domaine spécialisé)	-	1000 heures
LEAD AUDITOR	Provisional Auditor	-	-	-
	Auditor	2 ans (dont 1 dans le domaine spécialisé)	200 heures	-
	Lead Auditor	5 ans (dont 2 dans le domaine spécialisé)	300 heures	-
	Senior Lead Auditor	10 ans (dont 7 dans le domaine spécialisé)	1000 heures	-
LEAD IMPLEMENTER	Provisional Implementer	-	-	-
	Implementer	2 ans (dont 1 dans le domaine spécialisé)	-	200 heures
	Lead Implementer	5 ans (dont 2 dans le domaine spécialisé)	-	300 heures
	Senior Lead Implementer	10 ans (dont 7 dans le domaine spécialisé)	-	1000 heures
LEAD AUDITOR ET LEAD IMPLEMENTER	Master	20 ans (10 dans un rôle de leadership dans le domaine spécialisé)	10 000 heures combinant des activités d'audit et de projet	

Remarque : *Pour les programmes de certificat Foundation accrédités par l'ANAB, la participation à la formation correspondante est une exigence obligatoire.*

Confiance numérique : Sécuriser votre avenir

Les clients veulent savoir que leurs données sont en sécurité, et les entreprises doivent prouver qu'elles peuvent les protéger. La confiance numérique est la clé pour établir des relations solides et rester compétitif.

Qu'est-ce que la confiance numérique ?

La confiance numérique est la confiance que les personnes et les organisations accordent à votre environnement numérique. Cela signifie que vos systèmes, vos données et vos interactions sont sécurisés, fiables et exempts de menaces. La transformation numérique a permis aux organisations de divers secteurs d'atteindre une croissance durable et une productivité accrue. Une stratégie de transformation numérique efficace permet d'éviter les problèmes pendant la transition et après la mise en œuvre. Une transformation numérique réussie nécessite des technologies appropriées et des personnes compétentes.

Pourquoi la confiance numérique est-elle importante ?

Lorsque les clients vous font confiance, ils restent fidèles. La confiance numérique renforce la crédibilité, valorise votre marque et vous permet de garder une longueur d'avance sur vos concurrents. Il ne s'agit pas seulement de sécurité — mais aussi de croissance et de réussite.

PECB : Votre partenaire en confiance numérique

Chez PECB, nous proposons des programmes de certification de premier plan qui vous aident à instaurer, maintenir et démontrer la confiance numérique. Nos formations reconnues à l'échelle internationale couvrent tous les domaines, de la cybersécurité et de la protection des données au piratage éthique et à la transformation numérique.

Pourquoi choisir PECB ?

Avec PECB, vous acquérez les compétences et les certifications nécessaires pour diriger dans un monde axé sur le numérique. Nous permettons aux professionnels de sécuriser leurs organisations et d'instaurer la confiance auprès de leurs clients.

Formats de prestation des formations PECB

Les méthodes de prestation de PECB répondent aux besoins d'un large public d'apprenants, garantissant l'accessibilité, la flexibilité et la qualité du processus de formation et de certification.

En présentiel
Participez à des sessions directes et interactives avec des formateurs certifiés PECB dans un environnement d'apprentissage structuré en face à face, idéal pour l'application pratique des connaissances.

Classe virtuelle
Suivez des formations interactives et engageantes animées par des formateurs certifiés PECB dans une salle de classe virtuelle, accessibles à tous, y compris aux personnes ayant des contraintes de temps ou de déplacement

eLearning
Formations flexibles et indépendantes du lieu, accessibles via des vidéos préenregistrées. Propose des quiz et des lectures complémentaires.

Autoformation
Autoformation à votre rythme avec accès aux supports de formation. Idéal pour les personnes disposant déjà de connaissances préalables et n'ayant pas besoin d'un enseignement encadré.

Tim Rama
Directeur général de PECB

L'éducation est au cœur de ce que nous faisons chez PECB. Nous visons à cultiver les talents, à inspirer l'excellence et à placer la confiance numérique au centre de chaque expérience d'apprentissage. À mesure que les organisations et les individus s'appuient de plus en plus sur les systèmes numériques, nous fournissons les compétences nécessaires pour protéger l'information et créer des environnements sécurisés. Notre mission va au-delà des certifications et encourage l'apprentissage continu ainsi que le développement personnel. Nous croyons que le savoir crée des opportunités et nous souhaitons que les professionnels envisagent l'avenir sereinement, en adoptant le changement et en construisant leur réussite sur une base de confiance.

SÉCURITÉ DE L'INFORMATION ET CYBERSÉCURITÉ

Pourquoi la sécurité de l'information ?

La sécurité de l'information est essentielle, car elle protège les principes fondamentaux de la confidentialité, de l'intégrité et de la disponibilité des données.
Sans ces protections, les informations sensibles sont exposées à des risques pouvant avoir des conséquences pour les individus, les organisations et la société dans son ensemble.

Pourquoi la gestion de la cybersécurité ?

La gestion de la cybersécurité est nécessaire, car elle fournit l'orientation stratégique et le contrôle requis pour protéger les ressources numériques d'une organisation et assurer la continuité des opérations.

Pourquoi la cybersécurité technique ?

La cybersécurité technique est essentielle, car elle englobe les outils, technologies et méthodes qui protègent activement les systèmes et les données contre les cybermenaces.

ISO/IEC 27001 Information Security Management Systems

Présentation de la norme ISO/IEC 27001 et de son processus de certification

ISO/IEC 27001 définit les exigences applicables aux organisations souhaitant établir, mettre en œuvre, maintenir et améliorer en continu un système de management de la sécurité de l'information. La certification ISO/IEC 27001 représente une référence mondiale en matière de systèmes de management de la sécurité de l'information (SMSI). Cette certification guide les organisations dans la mise en œuvre d'une méthode structurée pour protéger les informations sensibles. Elle repose sur un cadre complet permettant d'identifier, d'évaluer et de traiter les risques liés à la sécurité de l'information, ce qui est essentiel pour préserver la confidentialité, l'intégrité et la disponibilité des données organisationnelles critiques.

Selon Gartner, Inc., les dépenses mondiales des utilisateurs finaux en matière de sécurité de l'information devraient atteindre 213 milliards de dollars américains en 2025 et augmenter davantage pour atteindre environ 240 milliards de dollars américains en 2026.

Avantages de la certification ISO/IEC 27001

- **Amélioration de la sécurité de l'information**
- **Meilleure gestion des risques**
- **Renforcement des compétences organisationnelles**
- **Accès à un réseau mondial d'experts en normes de sécurité**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27001 Foundation Acquérir des connaissances sur les composants fondamentaux nécessaires à la mise en œuvre et au management d'un SMSI basé sur la norme ISO/IEC 27001	2 JOURS
ISO/IEC 27001 Lead Implementer Développer les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et le maintien d'un SMSI basé sur la norme ISO/IEC 27001	5 JOURS
ISO/IEC 27001 Lead Auditor Acquérir les connaissances et compétences nécessaires pour réaliser un audit de SMSI en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS
ISO/IEC 27001 Transition Comprendre les différences entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022 et aider une organisation à planifier et à mettre en œuvre les changements nécessaires dans un SMSI existant conformément à la norme ISO/IEC 27001:2022	2 JOURS

S'inscrire

Depuis 2017, EduGroupe et PECB ont uni leurs expertises afin de soutenir les organisations et les professionnels dans l'acquisition de compétences à forte valeur ajoutée fondées sur la certification. Au fil des années, ce partenariat s'est imposé comme un modèle de coopération solide et visionnaire, au service de la sécurité, de la performance et de la responsabilité. Le partenariat entre EduGroupe et PECB repose sur une conviction commune : les compétences sont le moteur d'une transformation durable et sécurisée des entreprises. Dans un environnement où la conformité réglementaire, la protection des données et la responsabilité sociétale sont devenues essentielles, les deux entités s'engagent à promouvoir une culture de conformité et de résilience.

Jérôme Belzacki
Président d'EduGroupe

ISO/IEC 27002 Information Security Controls

Présentation de la norme ISO/IEC 27002 et de son processus de certification

ISO/IEC 27002 est une norme reconnue à l'échelle mondiale qui fournit un guide robuste pour renforcer le management de la sécurité de l'information au sein des organisations. L'adhésion à la norme ISO/IEC 27002 démontre une expertise en sécurité de l'information et permet aux professionnels de faire face aux cybermenaces en constante évolution avec confiance. ISO/IEC 27002 joue un rôle clé en aidant les organisations à protéger leurs données sensibles, à respecter les obligations légales et réglementaires et à instaurer une culture de sécurité solide.

Selon Business Research Insights, le marché mondial des « Systèmes de management de la sécurité de l'information (SMSI) » était évalué à environ 69,65 milliards de dollars américains en 2024 et devrait atteindre 107,13 milliards de dollars américains d'ici 2033 (TCAC d'environ 4,9 %).

Avantages de la certification ISO/IEC 27002

- **Faire face aux cybermenaces émergentes**
- **Renforcer l'assurance des données**
- **Garantir la conformité réglementaire**
- **Protéger les données sensibles**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27002 Foundation Acquérir des connaissances sur les pratiques de management de la sécurité de l'information, y compris la sélection, la mise en œuvre et le management des contrôles basés sur la norme ISO/IEC 27002	2 JOURS
ISO/IEC 27002 Manager Développer les compétences nécessaires pour mettre en œuvre, gérer et communiquer des contrôles de sécurité de l'information basés sur la norme ISO/IEC 27002	3 JOURS
ISO/IEC 27002 Lead Manager Acquérir les connaissances et compétences nécessaires pour réaliser un audit de SMSI en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

PECB Chief Information Security Officer (CISO)

Présentation de PECB CISO et de son processus de certification

PECB CISO (Chief Information Security Officer) est une accréditation spécialisée destinée aux professionnels souhaitant occuper des postes de direction de haut niveau dans le management de la sécurité de l'information. Le parcours vers l'obtention de la certification CISO implique une exploration approfondie des aspects stratégiques et opérationnels du leadership en sécurité de l'information. Ce processus de certification couvre un programme complet incluant les politiques de cybersécurité, la gestion des risques, la réponse aux incidents, la conformité et la communication avec les parties prenantes.

Avantages de la certification CISO

- **Évolution de carrière**
- **Crédibilité et attractivité accrues sur le marché**
- **Connaissances approfondies**
- **Reconnaissance mondiale**

En savoir plus

Formation et objectifs d'apprentissage

PECB CISO Acquérir les connaissances, compétences et stratégies nécessaires pour diriger efficacement des programmes de sécurité de l'information	**5 JOURS**

S'inscrire

Partenaire Titanium de PECB depuis de nombreuses années, Oo2 Formations & Consulting apprécie particulièrement la réactivité et le professionnalisme de ses équipes.
PECB se distingue par la qualité de ses contenus, son sens de l'innovation et une politique de tarification claire et cohérente.
Nous apprécions également la qualité du support client, aussi bien en amont de la formation que dans le suivi post-formation, toujours traités avec efficacité et sens du service.
PECB est pour nous un partenaire fiable, engagé et essentiel au succès de nos dispositifs de formation

Lea JACKEL
Responsable Pôle Formation, Oo2 Formations & Consulting

EBIOS

Présentation d'EBIOS et de son processus de certification

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthodologie d'évaluation des risques reconnue, principalement utilisée en France et dans d'autres régions francophones. La certification EBIOS reconnaît l'expertise d'un individu dans la méthodologie d'évaluation des risques EBIOS. Cette certification démontre une capacité avérée à évaluer et à gérer efficacement les risques liés à la sécurité de l'information grâce à l'approche structurée fournie par EBIOS.

Avantages de la certification EBIOS

- **Évolution de carrière en sécurité de l'information**
- **Contribution à une sécurité robuste**
- **Reconnaissance de l'expertise**
- **Engagement envers des normes de sécurité élevées**

En savoir plus

Formation et objectifs d'apprentissage

EBIOS Risk Manager Comprendre les éléments et concepts de l'évaluation des risques liés à la sécurité de l'information et développer les compétences nécessaires pour réaliser avec succès de telles évaluations en utilisant la méthode EBIOS	**3 JOURS**

S'inscrire

ISO/IEC 27005 Information Security Risk Management

Présentation de la norme ISO/IEC 27005 et de son processus de certification

ISO/IEC 27005 établit une référence en matière de lignes directrices pour la gestion des risques liés à la sécurité de l'information. Cette norme fournit une approche méthodique permettant aux organisations d'identifier, d'évaluer et de gérer les risques associés à leurs actifs informationnels. La certification ISO/IEC 27005 est très importante pour les professionnels de la sécurité de l'information. Elle leur apporte les compétences nécessaires pour identifier les menaces, les vulnérabilités et leurs impacts, et pour prendre des décisions éclairées en matière de traitement des risques.making informed risk mitigation decisions.

Selon IBM, le coût moyen d'une violation de données en 2025 s'élevait à 4,4 millions de dollars américains

Avantages de la certification ISO/IEC 27005

- **Expertise dans la protection de l'information**
- **Adaptabilité face à l'évolution du paysage de la sécurité**
- **Décisions éclairées en matière de traitement des risques**
- **Identification des menaces et des vulnérabilités**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27005 Foundation Acquérir des connaissances sur l'interprétation des lignes directrices d'ISO/IEC 27005 afin d'identifier, d'évaluer et de gérer les risques liés à la sécurité de l'information	2 JOURS
ISO/IEC 27005 Risk Manager Développer les compétences nécessaires pour réaliser des processus de gestion des risques liés aux actifs de sécurité de l'information en suivant les lignes directrices d'ISO/IEC 27005	3 JOURS
ISO/IEC 27005 Lead Risk Manager Acquérir l'expertise nécessaire pour accompagner une organisation dans la réalisation des processus de gestion des risques liés à la sécurité de l'information en se référant aux lignes directrices de la norme ISO/IEC 27005	5 JOURS

S'inscrire

En tant que responsable des achats chez Global Knowledge, je travaille avec PECB depuis plus de 12 ans maintenant. Un partenariat irréprochable au fil de toutes ces années grâce à leur grand professionnalisme et à leur réactivité. Leurs formations sont de grande qualité et alignées sur les besoins du marché, et leurs certifications sont reconnues pour leur rigueur et leur valeur sur le marché.

Selim Zeggai
Global Knowledge, France

ISO/IEC 27035 Information Security Incident Management

Présentation de la norme ISO/IEC 27035 et de son processus de certification

ISO/IEC 27035 est une norme internationale qui fournit des lignes directrices pour la gestion des incidents de sécurité de l'information. La certification ISO/IEC 27035 est une qualification essentielle pour les professionnels souhaitant maîtriser la gestion des incidents de sécurité de l'information. Cette certification est conçue pour valider et renforcer vos compétences en matière d'identification, de gestion et de prévention efficaces des incidents de sécurité au sein de toute organisation.

Selon Business Research Insights, la taille du marché mondial de la réponse aux incidents est évaluée à 29,7a milliards de dollars américains en 2025 et devrait atteindre environ 148.a1 milliards de dollars américains d'ici 2035, avec un taux de croissance annuel composé (TCAC) estimé à environ 17,3 % sur la période 2025-2035.

Avantages de la certification ISO/IEC 27035

- **Réponse efficace aux incidents**
- **Renforcement de la sécurité organisationnelle**
- **Reconnaissance mondiale**
- **Amélioration des compétences et des connaissances en TI**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27035 Foundation Acquérir des connaissances sur les principaux éléments de la mise en œuvre d'un plan de gestion des incidents de sécurité et sur la gestion des incidents de sécurité de l'information	2 JOURS
ISO/IEC 27035 Lead Incident Manager Acquérir les compétences et les connaissances nécessaires pour accompagner une organisation dans la mise en œuvre et le management d'un plan de gestion des incidents de sécurité de l'information conformément aux lignes directrices d'ISO/IEC 27035	5 JOURS

S'inscrire

ISO/IEC 27034 Application Security

Présentation de la norme ISO/IEC 27034 et de son processus de certification

La certification ISO/IEC 27034 Application Security permet aux professionnels d'acquérir des compétences avancées pour le management du programme de sécurité des applications fondé sur les normes ISO/IEC 27034.

L'obtention de la certification ISO/IEC 27034 Application Security implique une formation approfondie couvrant la conformité légale, la gestion des risques et l'intégration de la sécurité tout au long du cycle de vie du développement des applications, jusqu'au déploiement et à la maintenance. Ce processus de certification développe votre capacité à identifier et à atténuer les risques de sécurité, vous préparant ainsi à des rôles de leadership en sécurité informatique.

Avantages de la certification ISO/IEC 27034

- **Renforcement de l'expertise dans un domaine essentiel de la sécurité informatique**
- **Perspectives de carrière de haut niveau en cybersécurité**
- **Leadership stratégique**
- **Développement professionnel**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27034 Foundation Acquérir des connaissances sur les principaux éléments de la sécurité des applications selon la norme ISO/IEC 27034	2 JOURS
ISO/IEC 27034 Lead Application Security Implementer Acquérir les compétences nécessaires pour diriger et mettre en œuvre un programme de sécurité des applications conformément à la norme ISO/IEC 27034	5 JOURS
ISO/IEC 27034 Lead Application Security Auditor Acquérir les connaissances et les compétences nécessaires pour réaliser un audit de la sécurité des applications en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

ISO/IEC 27400 IoT Security and Privacy

Présentation de la norme ISO/IEC 27400 et de son processus de certification

La certification ISO/IEC 27400 atteste de l'expertise en matière de management de la sécurité et de la protection de la vie privée des systèmes et services IoT. L'obtention de la certification ISO/IEC 27400 nécessite la maîtrise des défis spécifiques liés à la sécurité des systèmes IoT. Cette certification évalue votre capacité à protéger les organisations contre les menaces, en mettant l'accent sur la protection de la vie privée des utilisateurs et sur la nature distribuée de l'IoT. Elle est de plus en plus essentielle pour les professionnels du management des systèmes IoT afin de prouver une compréhension approfondie des risques associés et la capacité à les atténuer.associated risks.

Avantages de la certification ISO/IEC 27400

- **Expertise en sécurité IoT**
- **Compétences en matière d'atténuation des risques**
- **Valorisation du profil professionnel**
- **Capacité à gérer les défis de sécurité de l'IoT**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27400 Foundation Acquérir des connaissances sur les principes fondamentaux de la sécurité et de la protection de la vie privée liés à l'IoT ainsi que sur la norme ISO/IEC 27400	2 JOURS
ISO/IEC 27400 Lead Manager Maîtriser le management des processus et des contrôles relatifs à la sécurité et à la protection de la vie privée des systèmes IoT selon la norme ISO/IEC 27400	5 JOURS

S'inscrire

Pourquoi choisir une carrière en sécurité de l'information ?

- → Demande croissante
- → Secteur en plein essor
- → Possibilités d'évolution

Carrières lucratives dans le domaine de la sécurité de l'information

Chief Information Security Officer (CISO)
Le CISO est un cadre de haut niveau chargé d'établir et de maintenir la vision, la stratégie et le programme d'une organisation afin de garantir que les actifs informationnels et les technologies soient correctement protégés.
Salaire annuel moyen : **U.S. $315,868**

Directeur de la sécurité de l'information
Supervise la stratégie globale de sécurité de l'information d'une organisation, en garantissant la confidentialité, l'intégrité et la disponibilité des données.
Salaire annuel moyen : **U.S. $216,812**

Responsable de la sécurité de l'information
Ce poste se concentre sur la gestion et la supervision de l'ensemble du programme de sécurité de l'information d'une organisation. Salaire annuel moyen : **U.S. $187,221**

Architecte de sécurité
Un architecte de sécurité conçoit, met en place et supervise la mise en œuvre de la sécurité des réseaux et des systèmes informatiques d'une organisation.
Salaire annuel moyen : **U.S. $204,664**

Analyste en sécurité de l'information
Protège les systèmes informatiques et les réseaux d'une organisation en identifiant et en résolvant les problèmes de sécurité potentiels et avérés. Salaire annuel moyen : **U.S. $160,292**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Nous sommes ravis de contribuer au catalogue de formations PECB 2026. Notre partenariat avec PECB est d'une qualité exceptionnelle ; nous apprécions tout particulièrement la réactivité, la disponibilité et l'attention constante des équipes de PECB. Les retours de nos clients et candidats sont excellents, tant en ce qui concerne la qualité des formations que le suivi et l'accompagnement fournis. Pour nous, ce partenariat représente une réelle valeur ajoutée, fondée sur la confiance et le professionnalisme, avec des services et des contenus parfaitement adaptés aux besoins du marché et de nos clients — toujours portés par l'innovation et l'amélioration continue.

Carine de Freitas
Directrice d'agence chez M2i Formation

Gestion de la cybersécurité

Présentation de la gestion de la cybersécurité et de son processus de certification

La gestion de la cybersécurité désigne le processus de supervision et de coordination des efforts visant à protéger les systèmes informatiques, les réseaux et les données d'une organisation contre les attaques numériques, les accès non autorisés ou les dommages. S'engager dans une certification en gestion de la cybersécurité constitue une étape déterminante pour devenir un leader compétent dans le domaine de la sécurité numérique. Cette certification s'adresse aux professionnels qui souhaitent acquérir une compréhension approfondie et des compétences pratiques pour superviser et piloter les stratégies de cybersécurité au sein des organisations.

Selon Fortune Business Insights, le marché mondial de la cybersécurité était évalué à environ 193,73 milliards de dollars américains en 2024 et devrait atteindre environ 218,98 milliards de dollars américains en 2025, puis environ 562,77 milliards de dollars américains d'ici 2032 (TCAC ≈ 14,4 %).

Avantages de la certification en gestion de la cybersécurité

- **Renforcement de l'expertise en sécurité numérique**
- **Amélioration des compétences en leadership**
- **Meilleure prise de décision**
- **Compréhension élargie de l'évaluation des risques**

En savoir plus

Formation et objectifs d'apprentissage	
Cybersecurity Foundation Acquérir des connaissances sur les principaux éléments des principes et concepts de la cybersécurité alignés sur les bonnes pratiques du secteur, notamment la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST	2 JOURS
Lead Cybersecurity Manager Acquérir les compétences et les connaissances nécessaires pour accompagner une organisation dans la mise en œuvre, le management et l'amélioration continue des programmes de cybersécurité	5 JOURS

S'inscrire

Cloud Security

Présentation de la sécurité du cloud et de son processus de certification

La certification Cloud Security est une accréditation professionnelle qui valide l'expertise en matière de conception, de mise en œuvre et de management d'infrastructures et de services cloud sécurisés. Le parcours menant à l'obtention d'une certification Cloud Security implique la maîtrise des complexités du cloud computing et de ses défis en matière de sécurité. Ce processus de certification vous forme aux différents modèles de services cloud (IaaS, PaaS, SaaS), aux types de déploiement cloud (public, privé, hybride), ainsi qu'aux considérations de sécurité propres à chacun.

Avantages de la certification Cloud Security

- **Compétences spécialisées**
- **Pertinence dans le domaine en pleine croissance de la sécurité du cloud**
- **Amélioration de l'employabilité**
- **Renforcement de la sécurité de l'emploi**

En savoir plus

Formation et objectifs d'apprentissage

Lead Cloud Security Manager Acquérir les compétences nécessaires pour planifier, mettre en œuvre, gérer et maintenir un programme de sécurité du cloud fondé sur les normes ISO/IEC 27017 et ISO/IEC 27018	**5 JOURS**

S'inscrire

Penetration Testing

Présentation du Penetration Testing et de son processus de certification

La certification Penetration Testing est une accréditation professionnelle qui démontre une expertise dans l'évaluation et l'exploitation des vulnérabilités des systèmes informatiques et des réseaux afin d'en renforcer la sécurité. Le parcours menant à l'obtention de la certification Penetration Testing repose sur une exploration approfondie des techniques de piratage éthique et d'évaluation de la sécurité. Ce parcours de certification vous apprend à penser comme un attaquant et à utiliser ces connaissances pour identifier et corriger les vulnérabilités de sécurité.

Avantages de la certification Penetration Testing

- **Engagement envers la cybersécurité**
- **Potentiel de rémunération plus élevé**
- **Développement professionnel**
- **Démonstration de compétences en piratage et en identification des vulnérabilités**

En savoir plus

Formation et objectifs d’apprentissage

Lead Pen Test Professional

Acquérir les connaissances et les compétences nécessaires pour diriger un test d’intrusion professionnel en combinant des techniques pratiques et des compétences en management afin d’analyser les résultats du test

5 JOURS

S’inscrire

Sécurité SCADA

Présentation du SCADA et de son processus de certification

SCADA (Supervisory Control and Data Acquisition) est un système utilisé pour surveiller et contrôler à distance les processusindustrielsetlesinfrastructures. Ce parcours de certification vous dote des compétences et des connaissances spécialisées essentielles pour sécuriser les systèmes SCADA, qui jouent un rôle clé dans le contrôle industriel et les infrastructures critiques.
La certification couvre notamment la compréhension des architectures des systèmes SCADA, l'identification et l'atténuation des vulnérabilités, la mise en œuvre de protocoles de sécurité robustes et la réponse efficace aux cybermenaces potentielles.

Avantages de la certification SCADA

- **Amélioration de la mise en œuvre de la sécurité**
- **Approche professionnelle globale de la sécurité**
- **Renforcement des connaissances en sécurité SCADA**
- **Approche holistique de la sécurité**

En savoir plus

Formation et objectifs d'apprentissage	
Lead SCADA Security Manager Développer les compétences nécessaires pour mettre en œuvre efficacement un programme de sécurité SCADA protégeant les systèmes contre les menaces, les vulnérabilités et les risques	5 JOURS

S'inscrire

ISO/IEC 27033 Networking Security

Présentation de la norme ISO/IEC 27033 et de son processus de certification

La certification en sécurité des réseaux constitue une reconnaissance formelle de l'expertise en matière de protection de l'infrastructure réseau et des données contre différents types de cybermenaces et de vulnérabilités, et garantit la confidentialité, l'intégrité et la disponibilité. Le parcours vers l'obtention d'une certification en sécurité des réseaux implique une exploration approfondie des concepts, approches, méthodes et techniques liés à la mise en œuvre et au management efficace de la sécurité des réseaux, ainsi que de l'interprétation des lignes directrices de la série de normes ISO/IEC 27033. Ce parcours de certification couvre un programme complet, incluant des lignes directrices pour la conception et la mise en œuvre de la sécurité des réseaux, ainsi que l'utilisation de passerelles, de VPN et de l'accès réseau IP sans fil afin de sécuriser les communications entre les réseaux.

Avantages de la certification ISO/IEC 27033

- **Valorisation de la carrière en informatique et en cybersécurité**
- **Préparation aux défis complexes**
- **Crédibilité professionnelle renforcée**
- **Meilleure attractivité sur le marché**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27033 Lead Network Security Manager Acquérir les compétences nécessaires pour planifier, mettre en œuvre, gérer et maintenir la sécurité des réseaux conformément à la série de normes ISO/IEC 27033	5 JOURS

S'inscrire

Notre collaboration avec PECB a été véritablement exceptionnelle. Le soutien apporté par l'équipe de PECB se distingue par sa grande réactivité et son professionnalisme, et son personnel est toujours aimable et accessible. La conférence PECB à Barcelone était remarquablement organisée — elle a offert de précieuses opportunités d'apprentissage ainsi que des expériences de réseautage exceptionnelles. Les retours de nos participants aux formations ont été extrêmement positifs, en particulier concernant la qualité des supports de formation, l'expertise des formateurs, ainsi que les processus d'examen et de certification. Nous sommes fiers d'être partenaire de PECB et nous nous réjouissons à l'idée de poursuivre cette coopération fructueuse dans les années à venir.

Bojan Varga
Responsable du développement chez SIQ Ljubljana

Certification CMMC (Cybersecurity Maturity Model certification)

Présentation du CMMC et de son processus de certification

La certification Cybersecurity Maturity Model (CMMC) est une norme unifiée de cybersécurité intégrant les bonnes pratiques issues de divers cadres de référence. Elle comprend cinq niveaux de maturité adaptés aux organisations du secteur de la base industrielle de défense (Defense Industrial Base – DIB), le niveau requis dépendant du type d'informations traitées. S'engager dans un parcours de certification CMMC implique de comprendre et de mettre en œuvre un ensemble de pratiques et de processus de cybersécurité alignés sur le niveau de maturité que votre organisation vise à atteindre. Le processus de certification comprend cinq niveaux de maturité, allant d'une hygiène informatique de base à une hygiène avancée.

Selon IBM, le coût moyen des violations de données aux États-Unis a atteint un niveau record de 10,22 millions de dollars américains en 2025, soit une augmentation de 9 % par rapport à l'année précédente.

Avantages de la certification CMMC

- **Connaissances avancées en cybersécurité**
- **Expertise en conformité**
- **Reconnaissance sectorielle**
- **Évolution de carrière en cybersécurité**

En savoir plus

Formation et objectifs d'apprentissage	
CMMC Foundations Apprendre les concepts fondamentaux et les principes du modèle CMMC	2 JOURS
Certified CMMC Professional (CCP) Acquérir les connaissances et les compétences nécessaires pour interpréter, mettre en œuvre et gérer les pratiques CMMC conformément au modèle CMMC, et évaluer les pratiques du niveau 1 du CMMC	4 JOURS

S'inscrire

Remarque : CMMC Foundations est une formation PECB qui n'est pas approuvée par le Cyber-AB ; par conséquent, l'attestation PECB CMMC Foundations n'est pas une certification CMMC. À ce titre, cette attestation ne remplace pas une certification CMMC, ne la complète pas et ne constitue pas une étape vers l'obtention d'une certification CMMC.

DIRECTIVE NIS 2

Présentation de la directive NIS 2 et de son processus de certification

La certification relative à la directive NIS 2 concerne la conformité à la directive révisée de l'Union européenne sur la sécurité des réseaux et des systèmes d'information, en mettant l'accent sur le renforcement de la cybersécurité dans divers secteurs. La mise en conformité avec la directive NIS 2 nécessite une compréhension approfondie des réglementations et normes mises à jour en matière de sécurité des réseaux et des systèmes d'information au sein de l'Union européenne. Ce processus inclut l'identification et la mise en œuvre des mesures nécessaires pour protéger les infrastructures et services critiques contre les cybermenaces. Le parcours de certification couvre la gestion des risques, la déclaration des incidents et l'adoption de protocoles de sécurité appropriés.

Avantages de la certification NIS 2

- **Conformité aux normes de l'Union européenne**
- **Engagement renforcé en matière de cybersécurité**
- **Crédibilité accrue**
- **Expertise dans les secteurs critiques**

En savoir plus

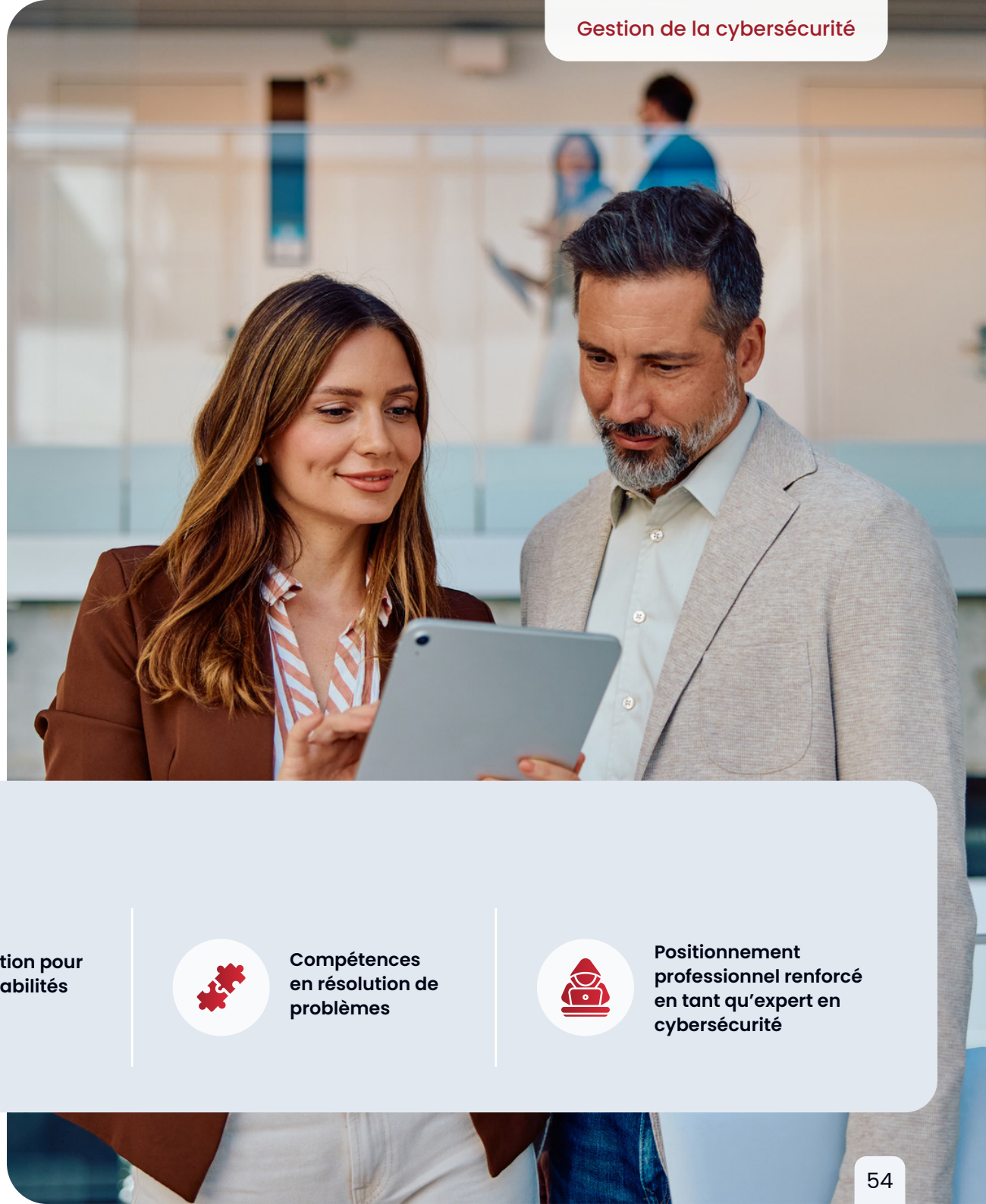
Formation et objectifs d’apprentissage	
NIS 2 Directive Foundation Comprendre les concepts fondamentaux nécessaires pour accompagner les organisations dans les phases initiales de planification, de mise en œuvre et de management des programmes de cybersécurité	2 JOURS
NIS 2 Directive Lead Implementer Acquérir les compétences essentielles pour aider les organisations à développer, mettre en œuvre, gérer et maintenir efficacement un programme de cybersécurité conforme aux exigences de la directive NIS 2	5 JOURS

S’inscrire

SOC 2

Présentation du SOC 2 et de son processus de certification

La certification SOC 2 est un titre professionnel qui reconnaît l'expertise en cybersécurité, en mettant l'accent sur les cinq principes de confiance : sécurité, disponibilité, intégrité du traitement, confidentialité et protection de la vie privée. S'engager dans le parcours pour devenir analyste certifié SOC 2 constitue une étape importante pour renforcer votre rôle dans le domaine de la cybersécurité. Ce parcours de certification implique l'acquisition de connaissances approfondies sur les cinq principes de confiance du SOC, ainsi que l'expertise nécessaire pour protéger la confidentialité des données des clients à l'aide des mesures définies par le SOC 2 afin de contrer les menaces.



Avantages de la certification SOC 2

- **Expertise en évaluation de la sécurité**
- **Préparation pour responsabilités élevées**
- **Compétences en résolution de problèmes**
- **Positionnement professionnel renforcé en tant qu'expert en cybersécurité**

En savoir plus

Formation et objectifs d'apprentissage

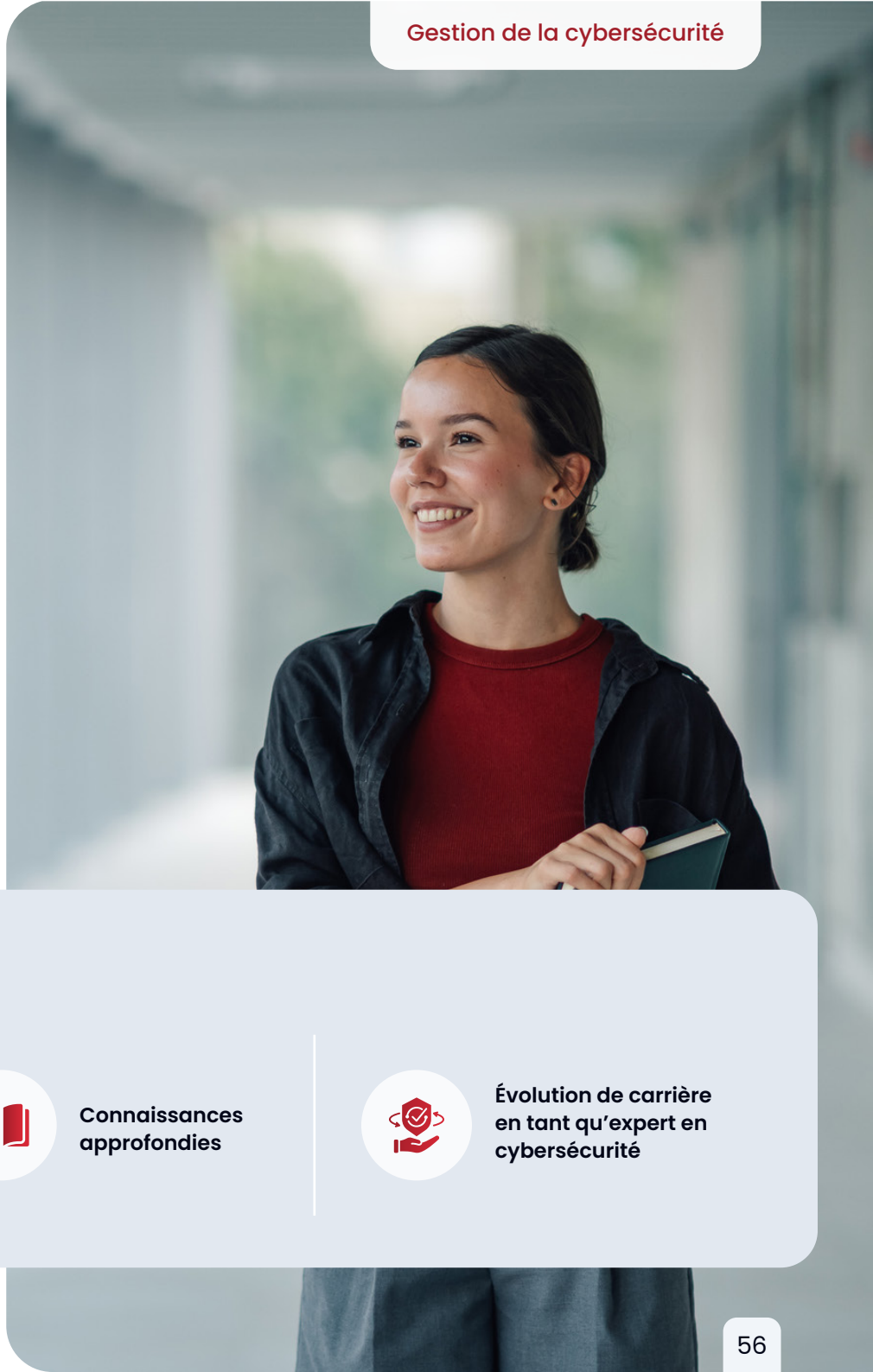
Lead SOC 2 Analyst Maîtriser la mise en œuvre et le management du cadre SOC 2 afin d'assurer la conformité de l'organisation en matière de protection et de sécurité des données	**5 JOURS**

S'inscrire

NIST Cybersecurity

Présentation du NIST Cybersecurity et de son processus de certification

La certification NIST Cybersecurity permet aux professionnels d'acquérir l'expertise nécessaire pour appliquer les cadres, lignes directrices et bonnes pratiques de cybersécurité largement reconnus du NIST. Elle se concentre sur la gestion des risques de sécurité, le renforcement de la protection de la vie privée et l'alignement sur le cadre de cybersécurité du NIST (CSF). Les orientations plus larges du NIST, notamment les publications spéciales clés telles que SP 800-12 (principes de sécurité), SP 800-53 (contrôles de sécurité et de protection de la vie privée), SP 800-37 (gestion des risques) et SP 800-171 (protection des informations contrôlées non classifiées), renforcent davantage la capacité d'une organisation à bâtir une posture de sécurité robuste. La maîtrise de ces ressources vous confère un avantage concurrentiel, vous permettant d'évoluer avec assurance dans le paysage de la cybersécurité et de soutenir le développement d'environnements numériques résilients et sécurisés.



Avantages de la certification NIST Cybersecurity

- **Solutions de cybersécurité adaptées**
- **Expertise en évaluation des menaces**
- **Connaissances approfondies**
- **Évolution de carrière en tant qu'expert en cybersécurité**

En savoir plus

Formation et objectifs d'apprentissage	
NIST Cybersecurity Foundation Acquérir des connaissances sur les principes fondamentaux et les concepts clés de la cybersécurité, fondés sur les normes de cybersécurité du NIST, nécessaires pour comprendre les concepts de gestion des risques et les mécanismes de contrôle qui soutiennent la protection des systèmes d'information et des données.	**2 JOURS**
NIST Cybersecurity Professional Maîtriser l'application des lignes directrices du NIST ainsi que le management des contrôles et des risques de cybersécurité	**5 JOURS**

S'inscrire

ISA/IEC 62443

Présentation de la norme ISA/IEC 62443 et de son processus de certification

La certification ISA/IEC 62443 valide l'expertise en cybersécurité des systèmes d'automatisation et de contrôle industriels (IACS), fondée sur les seules normes reconnues à l'échelle mondiale dédiées à la sécurisation des environnements de technologies opérationnelles. L'obtention de cette certification offre une exploration structurée du cadre ISA/IEC 62443, incluant les exigences de gouvernance, les contrôles de sécurité des systèmes et des composants, les méthodes d'évaluation des risques et les principes d'ingénierie « secure by design ». Ce parcours de certification dote les participants des compétences nécessaires pour évaluer les risques IACS, concevoir des architectures sécurisées, gérer les pratiques de sécurité tout au long du cycle de vie et aligner les fournisseurs et intégrateurs sur les attentes du secteur, permettant ainsi aux organisations de renforcer leur résilience dans divers secteurs industriels.

Avantages de la certification ISA/IEC 62443

- **Compétences démontrées en cybersécurité industrielle**
- **Capacité à réaliser des évaluations des risques IACS**
- **Compétence dans la conception de systèmes industriels sécurisés dès la conception**
- **Capacité renforcée à maintenir et améliorer la sécurité des IACS**
- **Amélioration de l'évaluation des fournisseurs et des prestataires de services**
- **Adaptation efficace des principes de sécurité informatique aux environnements OT**
- **Amélioration de la communication entre les parties prenantes grâce à un langage de normes unifié**
- **Crédibilité professionnelle reconnue à l'échelle mondiale en matière de sécurité des IACS**

Nouvelle formation

Formation et objectifs d'apprentissage	
ISA/IEC 62443 Lead Implementer Acquérir les compétences nécessaires pour diriger et mettre en œuvre un programme de cybersécurité des systèmes d'automatisation et de contrôle industriels (IACS) conformément à la norme ISA/IEC 62443	**5 JOURS**

S'inscrire

Canadian Program for Cybersecurity Certification

Présentation du CP-CSC et de son processus de certification

Le Canadian Program for Cyber Security Certification (CP-CSC) aide les professionnels à développer une expertise solide et pratique en cybersécurité, applicable aux secteurs industriels canadiens et aux environnements réglementés par le gouvernement. Le programme est conçu pour offrir aux participants une compréhension claire des exigences canadiennes en matière de cybersécurité, des attentes en gestion des risques et des bonnes pratiques de sécurité. Grâce à cette certification, les apprenants explorent les principaux cadres canadiens, les principes de gouvernance, les méthodes d'évaluation et les approches « secure by design ».

Le programme permet aux professionnels d'identifier et de gérer les cyberrisques, de concevoir et de maintenir des environnements sécurisés, et d'assurer la conformité aux normes réglementaires et industrielles canadiennes. L'obtention du CP-CSC aide les individus et les organisations à renforcer leurs bases en cybersécurité et à répondre aux attentes du Canada en matière de sécurité numérique.

Avantages du CP-CSC

- **Compréhension avérée des normes et exigences canadiennes en cybersécurité**
- **Capacité à réaliser des évaluations de cybersécurité dans des contextes réglementaires canadiens**
- **Compétences pour concevoir et maintenir des systèmes sécurisés alignés sur les bonnes pratiques canadiennes**
- **Capacité améliorée à gérer et à réduire les cyberrisques au sein d'une organisation**
- **Meilleure évaluation de l'état de préparation des fournisseurs et partenaires en matière de sécurité**
- **lignement renforcé entre les opérations IT/OT et les exigences de conformité canadiennes**
- **Communication et coordination plus claires entre les équipes techniques et non techniques**
- **Reconnaissance en tant que professionnel de confiance en cybersécurité au Canada**

Disponible bientôt

Formation et objectifs d'apprentissage	
Certified Canadian Program for Cyber Security Officer Dote les futurs responsables cyber d'une compréhension claire des normes canadiennes, des méthodes d'évaluation et des tâches opérationnelles de sécurité essentielles pour soutenir les stratégies de protection des organisations	5 JOURS

Disponible bientôt

Pourquoi choisir une carrière en gestion de la cybersécurité ?

- → Domaine en évolution rapide
- → Rôle essentiel dans la protection des actifs numériques
- → Parcours professionnels variés

Carrières bien rémunérées en gestion de la cybersécurité

Consultant en cybersécurité
Fournit des conseils et une expertise aux organisations sur la manière de protéger leurs actifs numériques et leurs infrastructures.
Salaire annuel moyen : **U.S. $153,027**

Responsable de la réponse aux incidents
Dirige la réponse aux cyberattaques et aux violations de données, en gérant le processus de confinement et d'atténuation des impacts.
Salaire annuel moyen : **U.S. $120,000**

Ingénieur en cybersécurité
Développe et met en œuvre des mesures de sécurité afin de protéger les informations contre les pirates, les cyberattaques et d'autres vulnérabilités.
Salaire annuel moyen : **U.S. $158,002–$160,836**

Ingénieur en sécurité des réseaux
Se concentre sur la protection de l'infrastructure réseau d'une organisation contre les menaces et les attaques.
Salaire annuel moyen : **U.S. $161,521–$162,531**

Testeur d'intrusion
Les testeurs d'intrusion sont chargés de tester et de sécuriser les systèmes informatiques, les réseaux et les applications afin de prévenir les violations.
Salaire annuel moyen : **U.S. $152,323**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Travailler avec PECB a été une excellente expérience. Leurs programmes de formation sont exceptionnellement bien structurés, pratiques et alignés sur les normes du monde réel, rendant le développement professionnel à la fois engageant et efficace. Le soutien et la réactivité de l'équipe tout au long de la collaboration ont été remarquables, garantissant une expérience fluide et enrichissante du début à la fin.

Radu Dănilă

Responsable de la coordination des formations chez Noble Prog, Roumanie

Certified Lead Ethical Hacker (CLEH)

Présentation du CLEH et de son processus de certification

La certification Certified Lead Ethical Hacker (CLEH) fournit des exigences complètes aux professionnels souhaitant maîtriser, mettre en œuvre et améliorer en continu les méthodologies de piratage éthique. Cette certification s'adresse aux personnes qui cherchent à identifier, exploiter et atténuer efficacement les vulnérabilités de cybersécurité tout en respectant des normes éthiques. Elle dote les candidats de connaissances avancées et de compétences pratiques pour réaliser des évaluations de sécurité approfondies, comprendre les cybermenaces émergentes et élaborer des stratégies de défense proactives. En outre, la certification CLEH souligne l'importance de se tenir à jour des derniers outils, techniques et exigences réglementaires, permettant aux professionnels de relever les défis réels de la cybersécurité avec confiance et précision. Cette certification constitue une référence en matière d'expertise en piratage éthique, garantissant que les personnes certifiées peuvent protéger les écosystèmes numériques dans divers secteurs.

Avantages de la certification CLEH

- **Renforcement des compétences en sécurité offensive**
- **Expertise complète en piratage éthique**
- **Maîtrise des techniques avancées de piratage éthique**
- **Amélioration des capacités de résolution de problèmes**

En savoir plus

Formation et objectifs d’apprentissage

Certified Lead Ethical Hacker (CLEH) Acquérir les connaissances et les compétences nécessaires pour gérer un projet et une équipe de tests d’intrusion, ainsi que pour planifier et réaliser des tests d’intrusion internes et externes, conformément aux bonnes pratiques	**5 JOURS**

S’inscrire

Certified Cyber Threat Analyst (CCTA)

Présentation du CCTA et de son processus de certification

Le Certified Cyber Threat Analyst (CCTA) est conçu pour les professionnels de la cybersécurité souhaitant développer une expertise en détection avancée des menaces, en analyse et en atténuation. Cette formation dote les candidats de méthodologies et de cadres complets pour établir, mettre en œuvre, maintenir et améliorer en continu les capacités organisationnelles d'identification, d'évaluation et de neutralisation des cybermenaces évolutives. La certification CCTA représente une référence mondiale en matière d'analyse des cybermenaces et de réponse aux incidents. Cette certification guide les professionnels dans la mise en œuvre d'une approche structurée de protection des actifs organisationnels en intégrant le renseignement sur les menaces, la chasse proactive aux menaces et la gestion des incidents.

Avantages de la certification CCTA

- **Renforcement de la détection et de la réponse aux menaces**
- **Chasse proactive aux menaces**
- **Amélioration de la gestion des incidents**
- **Adoption de cadres avancés**

En savoir plus

Formation et objectifs d’apprentissage

Certified Cyber Threat Analyst (CCTA)

Développer l’expertise nécessaire pour mener de manière proactive la chasse aux cybermenaces en utilisant le renseignement sur les menaces et des techniques d’analyse comportementale. Acquérir des compétences pratiques pour évaluer les schémas d’attaque, suivre les acteurs de la menace et renforcer les opérations de sécurité grâce à des stratégies de défense proactive.

5 JOURS

S’inscrire

C'est un honneur d'être partenaire de PECB, un leader mondial de la formation ISO. Grâce à cette alliance, nous avons formé des dizaines de professionnels en Équateur à travers des formations de haut niveau dispensées par des formateurs comptant plus de 20 ans d'expérience. Nous avons constaté que, grâce à ces apprentissages, les participants ont développé des compétences pratiques qu'ils peuvent appliquer immédiatement au sein de leurs organisations, leur permettant de dépasser les objectifs et de créer un impact positif et durable. Un aspect particulièrement précieux de PECB est la mise à jour continue de ses supports, garantissant que le contenu est toujours aligné sur les évolutions des normes et les bonnes pratiques actuelles du secteur. Nous sommes fiers de faire partie de cette alliance mondiale d'excellence aux côtés de PECB.

Ramiro Pulgar
PDG chez Blue Hat Corporation, Équateur

Certified Digital Forensics Examiner (CDFE)

Présentation due Certified Digital Forensics Examiner et de son processus de certification

La formation Certified Digital Forensics Examiner (CDFE) est spécialement conçue pour doter les professionnels de l'expertise nécessaire à la réalisation d'investigations numériques complètes et fiables. Proposée par PECB, cette formation favorise la confiance numérique en enseignant aux participants les méthodologies et les bonnes pratiques permettant d'exécuter des processus d'informatique légale afin d'extraire, de préserver et d'analyser les preuves numériques avec précision et exactitude. Reconnue comme une référence mondiale en informatique légale, la certification CDFE fournit un cadre structuré pour l'investigation des cybercrimes et des incidents numériques. Cette certification garantit que les professionnels sont pleinement préparés à protéger l'intégrité, la confidentialité et la disponibilité des preuves numériques — une compétence essentielle dans le paysage numérique actuel en constante évolution.

Benefits of CDFE Certification

- **Accès à des outils et techniques avancés d'informatique légale**
- **Anticipation des menaces émergentes**
- **Amélioration des capacités de réponse aux incidents**
- **Connaissances pratiques des outils d'informatique légale**

En savoir plus

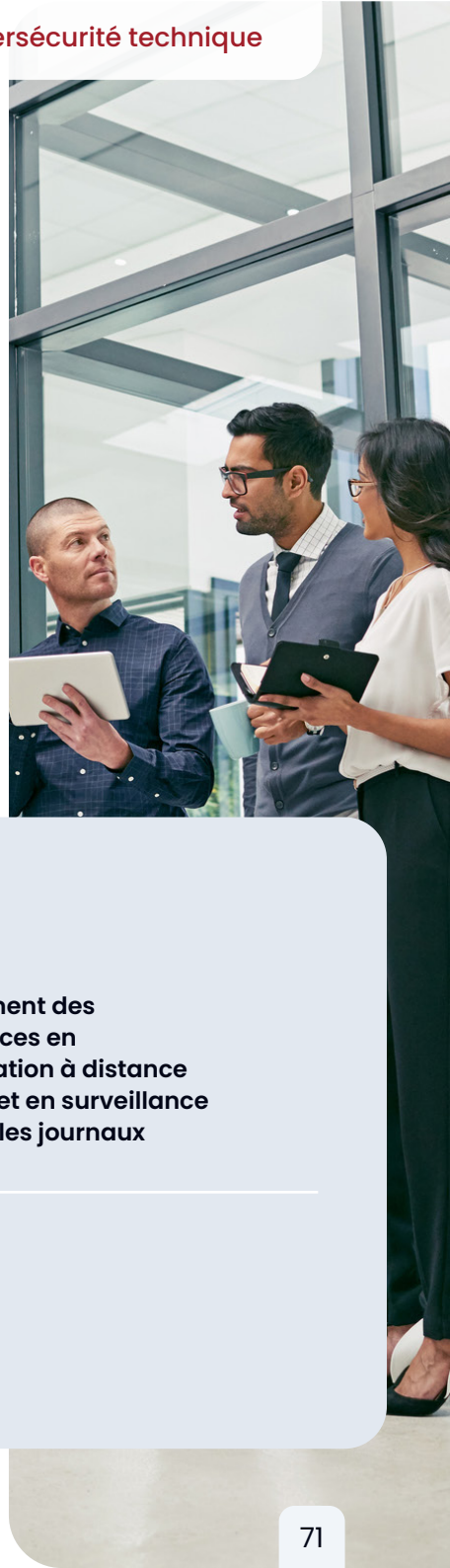
Formation et objectifs d'apprentissage	
Certified Digital Forensic Examiner (CDFE) Acquérir une expérience pratique grâce à des laboratoires techniques conçus pour vous apprendre à collecter, analyser et traiter les preuves numériques. Apprendre les techniques d'investigation numérique conformes aux normes du secteur ainsi que les exigences de conformité légale afin de soutenir la cybersécurité	**5 JOURS**

S'inscrire

Certified Linux Foundations (CLF)

Présentation du CLF et de son processus de certification

La formation Certified Linux Foundations (CLF) est destinée aux professionnels souhaitant acquérir une compréhension solide et pratique de Linux en tant que système d'exploitation moderne pour les environnements informatiques, cybersécurité et cloud. Cette formation propose un parcours structuré allant des concepts fondamentaux de Linux et de l'interaction en ligne de commande à la gestion des utilisateurs, des processus et des systèmes, en passant par l'administration à distance et les opérations axées sur la sécurité. Les participants exploreront la manière dont le noyau Linux, le shell et l'espace utilisateur interagissent, apprendront à naviguer dans le système de fichiers, à gérer les utilisateurs et les groupes, à contrôler les processus et les services, et à interpréter les journaux système à des fins opérationnelles et de sécurité.
Grâce à de nombreux travaux pratiques, ils mettront en œuvre des tâches concrètes telles que la gestion des fichiers, le scripting, l'authentification, la planification, le durcissement SSH et le durcissement de base des systèmes. L'obtention de cette certification démontre votre capacité à utiliser Linux avec assurance, à dépanner les problèmes courants et à exploiter des systèmes Linux sécurisés et fiables dans des environnements de production.



Avantages de la certification CLF

- **Acquisition d'une base pratique solide en Linux et en maîtrise de la ligne de commande**
- **Compréhension des concepts fondamentaux des utilisateurs, des processus, des services et des ressources système**
- **Renforcement des compétences en administration à distance sécurisée et en surveillance basée sur les journaux**
- **Meilleure préparation aux formations avancées en cybersécurité, DevOps et cloud**
- **Validation de votre capacité à maintenir, durcir et dépanner des systèmes Linux**

Nouvelle formation

Formation et objectifs d'apprentissage

Certified Linux Foundations (CLF)

CLF fournit une base pratique en Linux en enseignant la navigation en ligne de commande, la gestion des fichiers et des utilisateurs, le contrôle des logiciels et des processus, ainsi que les notions de base en réseau.
Les participants apprennent également les pratiques essentielles de sécurité, de journalisation et de dépannage nécessaires à l'exploitation et à la maintenance des systèmes Linux dans des environnements informatiques modernes.

5 JOURS

S'inscrire

Certified Advanced Penetration Tester (CAPT)

Présentation du Certified Advanced Penetration Tester et de son processus de certification

Le Certified Advanced Penetration Tester (CAPT) est une certification de niveau professionnel destinée aux experts en cybersécurité souhaitant perfectionner leurs compétences en piratage éthique et en tests d'intrusion. Ce programme dote les participants de l'expertise technique et de l'expérience pratique nécessaires pour simuler des attaques réelles et sécuriser des actifs critiques. Cette formation offre une compréhension approfondie des techniques et outils de pointe utilisés pour simuler des cyberattaques réelles sur les réseaux, les applications, les plateformes mobiles et les infrastructures cloud. Grâce à des sessions complètes animées par des formateurs et à des travaux pratiques, PECB garantit que les participants acquièrent une expérience concrète et la confiance nécessaire pour réaliser des tests d'intrusion complexes.

Avantages de la certification CAPT

- **Amélioration de la planification de la réponse aux incidents**
- **Maîtrise complète des techniques d'exploitation**
- **Maîtrise d'outils avancés de tests d'intrusion tels que Metasploit, Burp Suite Pro et Wireshark**
- **Compréhension approfondie des faiblesses de sécurité**

Nouvelle formation

Formation et objectifs d'apprentissage	
Certified Advanced Pen Test (CAPT) Acquérir l'expertise nécessaire pour réaliser des techniques avancées de tests d'intrusion, évaluer des infrastructures réseau complexes et exploiter les vulnérabilités. Développer des compétences pratiques en post-exploitation, en mouvements latéraux et en techniques d'évasion afin de renforcer les défenses de cybersécurité.	5 JOURS

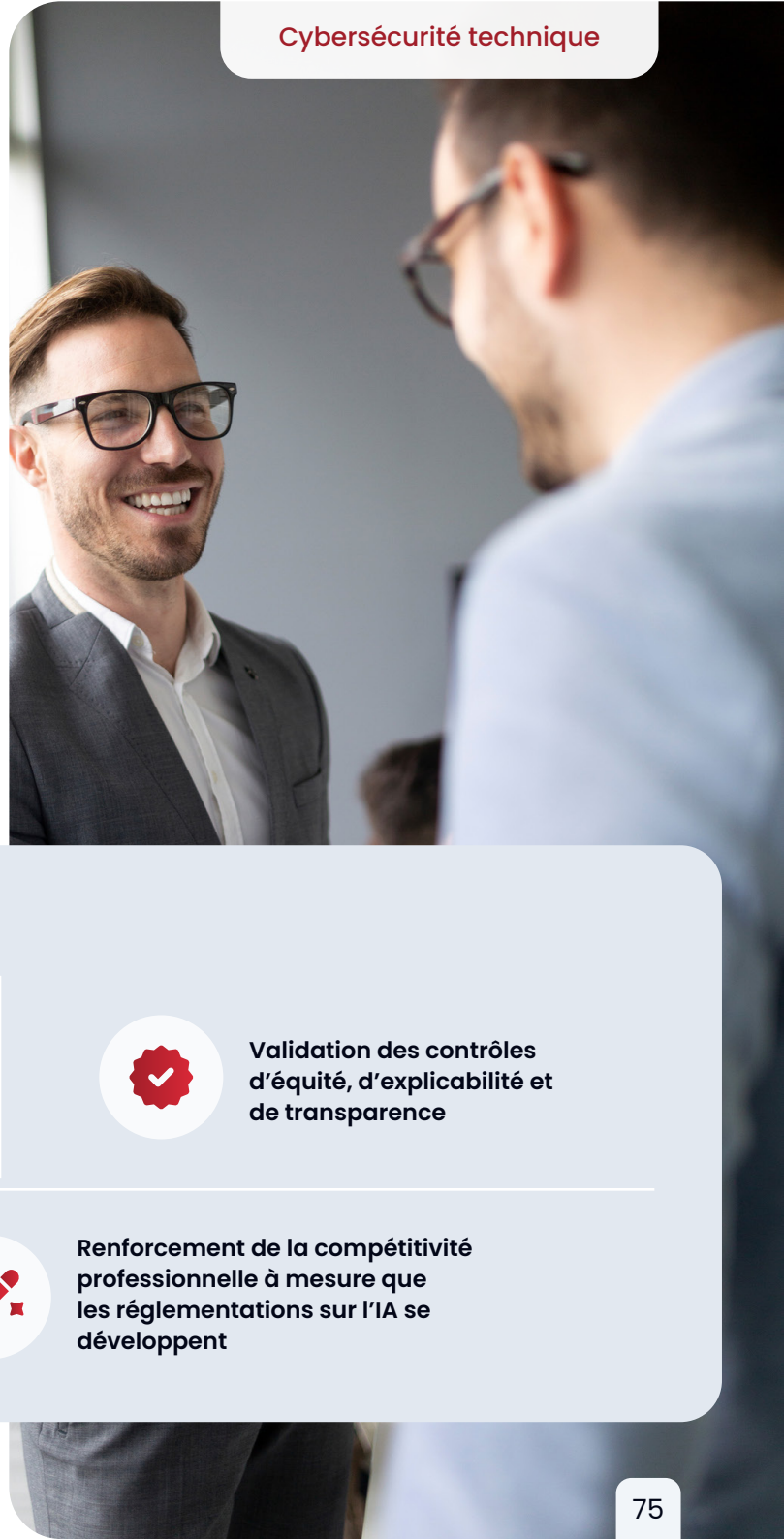
S'inscrire

Certified Artificial Intelligence Auditor (CAIA)

Présentation du CAIA et de son processus de certification

La formation Certified Artificial Intelligence Auditor (CAIA) propose une exploration complète de l'assurance de l'intelligence artificielle en vous guidant à travers les principes essentiels de l'audit, les cadres de conformité et les modèles de gouvernance. Vous apprendrez à évaluer les systèmes d'IA sous des angles éthique, technique, opérationnel et réglementaire afin de garantir la transparence, la responsabilité, l'équité et la sécurité tout au long du cycle de vie de l'IA.

Cette certification met l'accent sur l'évaluation de la qualité des données, de l'intégrité des modèles, des contrôles d'atténuation des biais, des pratiques de documentation et des exigences d'explicabilité. L'obtention de cette certification démontre votre capacité à planifier, réaliser et présenter les résultats d'audits d'IA soutenant une adoption de l'IA sûre, conforme, digne de confiance et responsable au sein des organisations.



Avantages de la certification CAIA

- **Renforcement de la supervision de la gouvernance et des risques liés à l'IA**
- **Garantie de la conformité aux réglementations et normes mondiales en matière d'IA**
- **Validation des contrôles d'équité, d'explicabilité et de transparence**
- **Amélioration de l'assurance d'audit pour une IA éthique et responsable**
- **Renforcement de la compétitivité professionnelle à mesure que les réglementations sur l'IA se développent**

Disponible bientôt

Formation et objectifs d'apprentissage

Certified Artificial Intelligence Auditor (CAIA) Prépare les professionnels à évaluer et auditer les systèmes d'IA en examinant les contrôles de gouvernance, les risques liés aux données et aux modèles, ainsi que la conformité aux exigences éthiques et réglementaires. Les participants apprennent des techniques pratiques d'assurance et de reporting qui permettent de garantir que les solutions d'IA sont transparentes, fiables et mises en œuvre de manière responsable.	5 JOURS

Disponible bientôt

Certified Cloud Security Analyst (CCSA)

Présentation du Certified Cloud Security Analyst et de son processus de certification

La formation Certified Cloud Security Analyst (CCSA) est conçue pour les professionnels de la cybersécurité chargés de sécuriser les charges de travail, les données et les identités dans des environnements cloud modernes. Cette formation propose un parcours structuré allant des concepts fondamentaux de la sécurité du cloud aux techniques défensives avancées, en combinant théorie et exercices pratiques. Vous apprendrez à évaluer les modèles de responsabilité partagée, à renforcer les configurations cloud, à sécuriser les identités et les accès, à protéger les données en transit et au repos, et à surveiller les infrastructures cloud natives afin de détecter les menaces et les erreurs de configuration.

Grâce à des travaux pratiques guidés, vous appliquerez ces compétences sur les principales plateformes cloud et dans des environnements conteneurisés. L'obtention de cette certification démontre votre capacité à analyser, détecter et répondre aux risques de sécurité du cloud tout en aidant les organisations à maintenir des architectures cloud résilientes et conformes.

Benefits of CCSA Certification

- **Développement d'une expertise pratique dans la sécurisation d'environnements multi-cloud et hybrides**
- **Renforcement de la protection des identités, des accès et des données dans le cloud**
- **Amélioration de la détection et de la réponse aux menaces à l'aide d'outils de surveillance cloud natifs**
- **Validation des compétences en durcissement des conteneurs, de Kubernetes et des services cloud`**
- **Davantage d'opportunités de carrière à mesure que l'adoption du cloud et les besoins en sécurité augmentent**

Disponible bientôt

Formation et objectifs d'apprentissage

Certified Cloud Security Analyst (CCSA)

5 JOURS

Dote les professionnels de la sécurité du cloud des compétences nécessaires pour sécuriser et surveiller les charges de travail dans des environnements cloud et conteneurisés à l'aide de l'IAM, de contrôles de protection des données et de configurations durcies.

Les participants mettent en pratique l'utilisation des outils cloud natifs de journalisation, de surveillance et d'investigation afin de détecter, analyser et atténuer les menaces dans des infrastructures cloud réelles.

Disponible bientôt

Certified SOC Analyst (CSOCA)

Présentation du CSOCA et de son processus de certification

La formation Certified SOC Analyst (CSOCA) est destinée aux professionnels responsables de la surveillance, de la détection et de la réponse aux événements de sécurité au sein d'un Security Operations Center (SOC). La formation couvre les concepts fondamentaux du SOC et des paysages de menaces, ainsi que les pratiques avancées de triage des alertes, d'investigation et de réponse aux incidents. Vous apprendrez à travailler efficacement avec des plateformes SIEM, à analyser les journaux et le trafic réseau, à enquêter sur des incidents de phishing et de malware, et à coordonner les activités de réponse avec les autres parties prenantes.

Grâce à des travaux pratiques guidés et à des scénarios basés sur des cas concrets, vous réaliserez des investigations de bout en bout, depuis l'alerte initiale jusqu'au confinement et à la reprise. L'obtention de cette certification démontre votre capacité à opérer en tant qu'analyste SOC capable d'identifier, de prioriser et de traiter des cybermenaces réelles de manière structurée et reproductible.

Avantages de la certification CCSA

- **Développement de compétences pratiques en surveillance SOC, triage des alertes et escalade**
- **Renforcement de la détection et de l'investigation des attaques de phishing, de malwares et de ransomwares**
- **Amélioration de la maîtrise des outils SIEM, d'analyse des journaux et de forensic réseau**
- **Optimisation de la coordination de la réponse aux incidents et du reporting au sein du SOC**
- **Davantage d'opportunités de carrière dans les opérations de sécurité et la détection des menaces**

Disponible bientôt

Formation et objectifs d'apprentissage

Certified SOC Analyst (CSOCA) Prépare les analystes à assurer les fonctions clés d'un SOC en surveillant les alertes, en analysant les journaux et les données des terminaux, et en enquêtant sur les incidents de phishing, de ransomware et autres incidents de sécurité. Les participants acquièrent une expérience pratique en triage des alertes, en corrélation, en forensic de base et en reporting des incidents afin de soutenir des opérations de sécurité efficaces de bout en bout.	5 JOURS

Disponible bientôt

Certified Elastic Stack Analyst (CESA)

Présentation du CESA et de son processus de certification

La formation Certified Elastic Stack Analyst (CESA) est conçue pour les professionnels de la sécurité qui utilisent l'Elastic Stack afin de détecter les menaces, mener des enquêtes et y répondre. Cette formation vous guide de la navigation dans Elasticsearch et Kibana à la création de visualisations, de recherches et d'alertes axées sur la sécurité pour soutenir les opérations quotidiennes d'un SOC. Vous apprendrez à déployer et gérer Elastic Agents et Beats, à collecter et normaliser les journaux et la télémétrie des terminaux, à exploiter Elastic Security, et à appliquer l'EQL et des analyses avancées pour la chasse aux menaces.

Grâce à des travaux pratiques, vous configurerez des règles de détection, enquêterez sur des incidents à l'aide de chronologies et de cas d'investigation, et intégrerez des capacités de protection des terminaux. L'obtention de cette certification valide votre capacité à utiliser Elastic comme plateforme d'analytique de sécurité et à transformer des données brutes en informations de sécurité exploitables.

Avantages de la certification CESA

- **Développement de compétences pratiques dans l'utilisation d'Elastic et de Kibana pour les opérations de sécurité**
- **Renforcement de la chasse aux menaces et de la détection grâce à l'EQL, aux analyses et aux règles de détection**
- **Amélioration de la collecte de télémétrie des journaux, des terminaux et du réseau à l'aide d'Elastic Agents et Beats**
- **Renforcement des processus d'investigation des incidents et de gestion des cas dans Elastic Security**
- **Davantage d'opportunités de carrière à mesure que les organisations adoptent l'Elastic Stack comme standard**

Disponible bientôt

Formation et objectifs d'apprentissage	
Certified Elastic Stack Analyst (CESA) Permet aux professionnels de la sécurité d'utiliser l'Elastic Stack comme plateforme d'analytique de sécurité en intégrant les données, en créant des tableaux de bord et en configurant des recherches et des alertes pour des cas d'usage clés. Les participants acquièrent une expérience pratique avec Elastic Security, les règles de détection, la chasse aux menaces basée sur l'EQL et les flux d'investigation afin de détecter les menaces, les analyser et y répondre efficacement.	5 JOURS

Disponible bientôt

Certified Web Application Security Analyst (CWASA)

Présentation du CWASA et de son processus de certification

La formation Certified Web Application Security Analyst (CWASA) est conçue pour les professionnels qui évaluent, sécurisent et surveillent les applications Web modernes et les API. Cette formation vous guide des concepts fondamentaux du HTTP et de l'architecture applicative jusqu'à l'analyse avancée des vulnérabilités Web courantes et émergentes. Vous apprendrez à identifier, exploiter et valider des failles telles que l'injection, l'authentification défaillante, l'exposition de données sensibles, les défaillances de contrôle d'accès, les erreurs de configuration de sécurité, le XSS, la désérialisation non sécurisée et les composants vulnérables.

Tout au long de la formation, vous réaliserez des travaux pratiques guidés simulant des scénarios réels d'attaque et de défense, incluant des recommandations de configuration sécurisée et de remédiation. L'obtention de cette certification démontre votre capacité à analyser les applications Web, à communiquer des constats techniques aux équipes de développement et à soutenir des pratiques de développement logiciel sécurisé tout au long du cycle de vie.

Avantages de la certification CWASA

- **Maîtrise de techniques pratiques pour identifier et exploiter les vulnérabilités des applications Web**
- **Renforcement des compétences en test de l'authentification, de l'autorisation et de la gestion des sessions**
- **Amélioration de la capacité à sécuriser les API, la gestion des données et la configuration applicative**
- **Fourniture de recommandations de remédiation concrètes et exploitables aux équipes de développement et DevOps**
- **Renforcement des perspectives de carrière en sécurité applicative, tests d'intrusion et développement sécurisé**

Disponible bientôt

Formation et objectifs d'apprentissage

Certified Web Application Security Analyst (CWASA)

5 JOURS

Dote les professionnels de la sécurité des compétences nécessaires pour évaluer la sécurité des applications Web et des API en analysant l'architecture, en cartographiant les surfaces d'attaque et en testant les vulnérabilités courantes telles que l'injection, le XSS et les défaillances de contrôle d'accès.

Les participants s'exercent à exploiter et valider les constats, à prioriser les risques et à recommander des améliorations de codage et de configuration sécurisés afin de soutenir le développement sécurisé et de protéger les actifs Web critiques.

Disponible bientôt

Certified Splunk Analyst (CSA)

Présentation du CSA et de son processus de certification

La formation Certified Splunk Analyst (CSA) est destinée aux professionnels de la sécurité et des opérations qui utilisent Splunk pour collecter, analyser et exploiter les données machines. Cette formation vous guide des concepts fondamentaux et la configuration de Splunk jusqu'aux flux avancés de recherche, de corrélation et de réponse aux incidents. Vous apprendrez à intégrer des sources de données, à créer des recherches et des tableaux de bord efficaces, à configurer des alertes et à exploiter les applications et modules complémentaires Splunk pour soutenir les opérations de sécurité.

Grâce à des travaux pratiques et à des exercices d'incidents réalistes, vous enquêterez sur des événements, effectuerez des analyses croisées des journaux et collaborerez aux activités de réponse en utilisant Splunk comme centre d'investigation central. L'obtention de cette certification démontre votre capacité à exploiter Splunk comme une puissante plateforme d'analytique et de réponse aux incidents, favorisant une détection et une remédiation rapides des menaces de sécurité.

Avantages de la certification CSA

- **Développement de compétences pratiques en recherche, visualisation et corrélation des données dans Splunk**
- **Amélioration de la détection et de l'investigation des incidents de sécurité à l'aide de tableaux de bord et d'alertes**
- **Renforcement de la capacité à intégrer et normaliser les journaux provenant de sources de données variées**
- **Amélioration de l'efficacité de la réponse aux incidents grâce aux playbooks, flux de travail et éléments de preuve dans Splunk**
- **Davantage d'opportunités de carrière dans les rôles SOC, de détection des menaces et d'ingénierie de la sécurité**

Disponible bientôt

Formation et objectifs d'apprentissage

Certified Splunk Analyst

Permet aux professionnels de la sécurité d'utiliser Splunk pour la surveillance de la sécurité et la réponse aux incidents en configurant les entrées de données, en créant des recherches SPL, des tableaux de bord et des alertes pour des cas d'usage clés.

Les participants acquièrent une expérience pratique dans la conduite d'investigations de bout en bout, la corrélation d'événements issus de multiples sources de données et la transformation des données machines en informations exploitables favorisant une détection, un triage et une réponse rapides.

5 JOURS

Disponible bientôt

Certified Cloud Incident Responder (CCIR)

Présentation du CCIR et de son processus de certification

La formation Certified Cloud Incident Responder (CCIR) est conçue pour les professionnels responsables de la détection, de l'analyse et de la résolution des incidents de sécurité dans des environnements cloud. Cette formation propose un parcours structuré allant des principes fondamentaux de la réponse aux incidents cloud jusqu'aux playbooks spécifiques aux plateformes AWS, Azure, Google Cloud, Microsoft 365 et Google Workspace. Vous apprendrez à préparer les environnements cloud à la gestion des incidents, à trier les alertes, à enquêter sur les identités et les charges de travail compromises, et à coordonner les activités de confinement et de reprise.

Grâce à des travaux pratiques, vous utiliserez des outils de sécurité cloud natifs, des journaux et de la télémétrie pour analyser des scénarios d'attaque réels et appliquer des procédures de réponse normalisées. L'obtention de cette certification démontre votre capacité à diriger et à exécuter des opérations de réponse aux incidents axées sur le cloud, permettant un rétablissement rapide des services tout en préservant les preuves et en respectant les exigences de conformité.

Avantages de la certification CCIR

- **Développement de compétences pratiques en réponse aux incidents sur les principales plateformes cloud**
- **Renforcement de la détection, du triage et de l'investigation des menaces basées sur le cloud**
- **Amélioration de l'utilisation des outils de sécurité cloud natifs, des journaux et de la télémétrie à des fins d'investigation**
- **Renforcement de la capacité à contenir, éradiquer et rétablir les environnements cloud compromis**
- **Davantage d'opportunités de carrière dans les opérations de sécurité cloud et la réponse aux incidents**

Disponible bientôt

Training Course and Learning Objectives

Certified Cloud Incident Responder

5 JOURS

Prépare les professionnels à gérer l'ensemble du cycle de réponse aux incidents dans des environnements cloud en préparant les comptes et les tenants, en analysant les journaux et en enquêtant sur les menaces liées aux identités, aux charges de travail, aux données et aux services SaaS.

Les participants acquièrent une expérience pratique dans l'exécution de playbooks sur AWS, Azure, Google Cloud, Microsoft 365 et Google Workspace, la documentation des constats, la coordination avec les parties prenantes et la mise en œuvre d'actions correctives afin de renforcer la résilience face aux incidents futurs.

Disponible bientôt

Pourquoi choisir une carrière en cybersécurité technique ?

- → Essentielle pour la confiance numérique et la protection des activités
- → Forte demande dans tous les secteurs
- → Parcours professionnels lucratifs et pérennes

Les professionnels de la cybersécurité technique jouent un rôle essentiel dans la protection des systèmes, des applications, des données et des technologies émergentes face à des cybermenaces de plus en plus sophistiquées. À mesure que les organisations accélèrent leur transformation numérique, la demande de spécialistes qualifiés en sécurité continue de croître à l'échelle mondiale.

Carrières bien rémunérées en cybersécurité technique

Certified Advanced Penetration Tester (CAPT)
Réalise des tests d'intrusion avancés et des exercices de type red team afin de simuler des cyberattaques réelles. Ce rôle se concentre sur l'exploitation de vulnérabilités complexes et le renforcement des défenses organisationnelles.
Salaire annuel moyen : **U.S. $132,900**

Certified Cloud Incident Responder (CCIR)
Intervient et gère les incidents de sécurité dans des environnements cloud, notamment les violations de données, les accès non autorisés, les infections par malwares et les erreurs de configuration.
Salaire annuel moyen : **U.S. $116,000**

Certified Cloud Security Analyst (CCSA)
Se concentre sur la sécurisation des infrastructures, des plateformes et des applications basées sur le cloud.
Ce rôle garantit la conformité, la gestion des risques et les contrôles de sécurité auprès des fournisseurs de services cloud tels qu'AWS, Azure et Google Cloud. Salaire annuel moyen : **U.S. $121,700**

Certified Elastic Stack Analyst (CESA)
Spécialisé dans l'utilisation de l'Elastic Stack (ELK) pour la détection des menaces, l'analyse des journaux et la surveillance de la sécurité. Les analystes Elastic soutiennent la détection, l'investigation et la réponse aux incidents grâce à des analyses avancées des données.
Salaire annuel moyen : **U.S. $118,500**

Certified Web Application Security Analyst (CWASA)
Responsable de l'identification, de l'analyse et de l'atténuation des vulnérabilités de sécurité dans les applications Web. Ce rôle se concentre sur les pratiques de codage sécurisé, les tests applicatifs et la protection contre des attaques telles que l'injection SQL, le XSS et le CSRF. Salaire annuel moyen : **U.S. $115,000**

Remarque : Les données salariales présentées ici proviennent de *Glassdoor* *et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Le partenariat avec PECB a renforcé ma crédibilité en tant que consultant, formateur et prestataire de formation. Leurs certifications accréditées garantissent à mes clients que je dispose de la formation, de l'expérience et des qualifications reconnues nécessaires pour les accompagner efficacement. Que je fournisse des services de conseil ou que je dispense des formations, les clients savent qu'ils bénéficient d'un accompagnement fiable et de haute qualité, soutenu par un organisme de certification reconnu à l'échelle mondiale. Grâce aux formats de formation flexibles de PECB, je suis en mesure de répondre à des besoins d'apprentissage variés tout en maintenant un haut niveau d'excellence. PECB se distingue par sa reconnaissance internationale, ses certifications accréditées, la conception pratique de ses formations, la diversité de ses modes de diffusion et son engagement envers l'excellence. Si vous souhaitez renforcer les compétences des professionnels et valoriser votre marque, PECB est le partenaire qu'il vous faut.

Michael Gross

Management System Certification Training Solutions - USA

CONTINUITÉ, RÉSILIENCE ET REPRISE

Pourquoi la continuité, la résilience et la reprise ?

La continuité, la résilience et la reprise sont essentielles pour permettre aux organisations de maintenir leurs activités lors de perturbations, de protéger les actifs critiques et de réduire les risques financiers et réputationnels. Ces stratégies renforcent l'adaptabilité, assurent une reprise rapide et favorisent la confiance des parties prenantes, positionnant les organisations sur la voie d'un succès durable dans

ISO 22301 Business Continuity Management System

Présentation de la norme ISO 22301 et de son processus de certification

ISO 22301 est une norme reconnue à l'échelle mondiale pour le management de la continuité des activités, garantissant que les organisations sont préparées à maintenir leurs opérations pendant et après un incident perturbateur. S'engager dans un parcours de certification ISO 22301 implique de maîtriser les principes de la continuité et de la résilience des activités. Ce processus de certification consiste à comprendre et à mettre en œuvre les bonnes pratiques pour développer, maintenir et améliorer un système de management de la continuité des activités (SMCA). Il couvre des domaines essentiels tels que l'évaluation des risques, la planification de la réponse aux incidents, l'analyse d'impact sur les activités et les stratégies de reprise.

Selon VynZ Research, le marché mondial du Business Continuity Management (BCM) était évalué à 1,62 milliard de dollars américains en 2025 et devrait atteindre 3,82 milliards de dollars américains d'ici 2035, avec un TCAC de 13,7 %.

Avantages de la certification ISO 22301

- **Expertise professionnelle en planification de la continuité et de la résilience des activités**
- **Opportunités de carrière**
- **Validation de la capacité de préparation organisationnelle**
- **Crédibilité renforcée en matière de continuité et de planification des activités**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 22301 Foundation Comprendre les principes, concepts et techniques essentiels d'un SMCA ainsi que les exigences de la norme ISO 22301	2 JOURS
ISO 22301 Lead Implementer Acquérir une compréhension approfondie des techniques de mise en œuvre d'un SMCA et apprendre à diriger une équipe dans la mise en œuvre d'un SMCA basé sur la norme ISO 22301	5 JOURS
ISO 22301 Lead Auditor Acquérir les connaissances et les compétences nécessaires pour auditer le SMCA d'une organisation par rapport aux exigences de la norme ISO 22301	5 JOURS

S'inscrire

Reprise après sinistre

Présentation de la reprise après sinistre et de son processus de certification

La certification Disaster Recovery est une accréditation professionnelle attestant de l'expertise en matière de planification, de mise en œuvre et de management des stratégies visant à restaurer les infrastructures et services TIC à la suite d'un sinistre. L'obtention d'une certification Disaster Recovery implique une exploration approfondie des méthodologies et des bonnes pratiques relatives à la restauration des services TIC après des événements perturbateurs. Ce parcours de certification couvre des domaines clés tels que l'évaluation des risques, l'analyse d'impact sur les activités, l'élaboration de stratégies de reprise et la mise en œuvre de plans de reprise après sinistre.

Selon Precedence Research, le marché mondial du « disaster recovery as a service » devrait passer de 22,40 milliards de dollars américains en 2025 à 195,71 milliards de dollars américains d'ici 2034, avec un TCAC de 27,23 % sur la période de prévision.

Avantages de la certification Disaster Recovery

- **Développement de compétences critiques**
- **Validation de l'expertise en mise en œuvre de stratégies de reprise après sinistre**
- **Protection des infrastructures**
- **Opportunités de carrière**

En savoir plus

Opportunités de carrière

Disaster Recovery Foundation Acquérir des connaissances sur les concepts clés d'un processus de planification de la reprise après sinistre des TIC	2 JOURS
Lead Disaster Recovery Manager Maîtriser les compétences requises pour aider les organisations à planifier, développer, mettre en œuvre et tester un processus de planification de la reprise après sinistre des TIC	5 JOURS

S'inscrire

PECB constitue une référence de premier plan en matière de développement professionnel dans le domaine de la GRC informatique, en proposant de manière constante des formations de haut niveau qui comblent l'écart entre la complexité des normes et leur application pratique. Son engagement en faveur de l'accessibilité mondiale est inégalé, avec une large gamme de modes de diffusion — de l'auto-apprentissage aux sessions interactives en direct — ainsi que des supports de formation disponibles en plusieurs langues afin de répondre à des styles d'apprentissage variés. En tant que partenaire engagé, nous sommes extrêmement reconnaissants pour l'écosystème collaboratif que PECB a su développer. Leur soutien indéfectible va bien au-delà de l'accréditation, en offrant les ressources et la réactivité nécessaires pour nous aider à nous développer et à servir efficacement notre marché local. Nous recommandons vivement un partenariat avec PECB à toute organisation à la recherche d'une relation fondée sur le succès mutuel, l'excellence opérationnelle et une vision commune visant à élever les normes industrielles à l'échelle mondiale.

Mostafa AlShamy
Egybyte

Digital Operational Resilience Act (DORA)

Présentation de DORA et de son processus de certification

La certification Digital Operational Resilience Act (DORA) démontre votre expertise dans la direction et la supervision de la mise en œuvre de stratégies de résilience opérationnelle numérique au sein des entités financières, afin de les aider à se conformer au Digital Operational Resilience Act (DORA) de l'Union européenne. Cette certification valide votre maîtrise de domaines tels que la gestion des risques TIC, la gestion des incidents, les tests de résilience opérationnelle numérique, la gestion des risques liés aux tiers, ainsi que le partage d'informations et de renseignements. Elle confirme votre capacité à satisfaire aux exigences techniques définies par DORA et vous positionne comme un professionnel de confiance capable de contribuer à la résilience opérationnelle des entités financières.

Avantages de la certification DORA

- **Amélioration des perspectives de carrière**
- **Capacité à naviguer dans des réglementations complexes**
- **Avantage concurrentiel**
- **Évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
DORA Foundation Comprendre les éléments fondamentaux du Digital Operational Resilience Act	2 JOURS
Lead DORA Manager Maîtriser la mise en œuvre et le management du cadre de résilience opérationnelle tel que défini par le Digital Operational Resilience Act	5 JOURS

S'inscrire

Crisis Management

Présentation de la gestion de crise et de son processus de certification

La certification en gestion de crise est un titre professionnel qui valide l'expertise en matière de planification, de gestion et de réponse efficace aux crises organisationnelles. L'obtention d'une certification en gestion de crise implique une analyse approfondie des stratégies et des compétences nécessaires pour gérer efficacement des situations imprévues et à forte pression au sein des organisations. Cette certification couvre des aspects essentiels de la gestion de crise, notamment l'évaluation des risques, la communication de crise, la prise de décision sous pression et les stratégies de reprise.

Avantages de la certification en gestion de crise

- **Compétences en atténuation des crises**
- **Expertise en communication de crise**
- **Amélioration du leadership et de la prise de décision**
- **Amélioration des perspectives de carrière**

En savoir plus

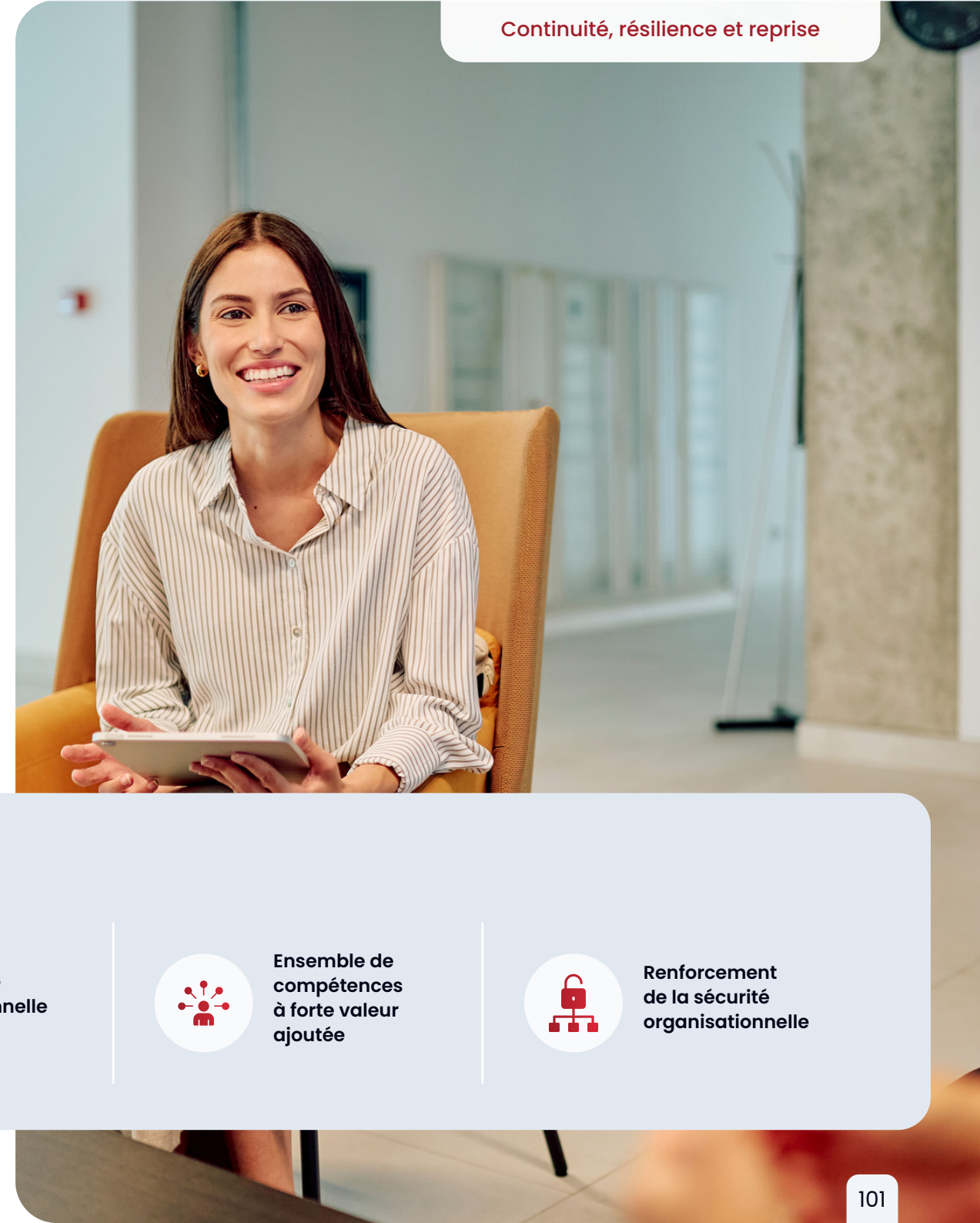
Formation et objectifs d'apprentissage	
Lead Crisis Manager Développer des compétences en planification, en mise en place et en amélioration continue des capacités stratégiques de gestion de crise	5 JOURS

S'inscrire

Gestion de la résilience opérationnelle

Présentation de la gestion de la résilience opérationnelle et de son processus de certification

La certification Operational Resilience Manager valide votre expertise dans la conception, le management et l'amélioration de cadres de résilience opérationnelle alignés sur les bonnes pratiques internationales. Cette certification démontre votre capacité à identifier, évaluer et atténuer les risques afin d'assurer la continuité des activités et la résilience opérationnelle. Elle reflète votre aptitude à concevoir des stratégies résilientes permettant de relever les défis complexes auxquels les organisations sont confrontées, en protégeant les opérations critiques et en favorisant une résilience durable.



Avantages de la certification en résilience opérationnelle

- **Maîtrise des mesures de résilience**
- **Crédibilité professionnelle accrue**
- **Ensemble de compétences à forte valeur ajoutée**
- **Renforcement de la sécurité organisationnelle**

En savoir plus

Formation et objectifs d’apprentissage

Lead Operational Resilience Manager

Maîtriser les compétences nécessaires pour piloter la résilience opérationnelle au sein de votre organisation, en garantissant des systèmes et des processus robustes capables de résister aux perturbations et de s’y adapter

5 JOURS

S’inscrire

Travailler avec PECB a été une expérience extrêmement enrichissante et à forte valeur ajoutée. Leur professionnalisme, leur réactivité et leur engagement envers la qualité ont grandement soutenu notre mission chez Aswar Akka Consultancy. Grâce à ce partenariat, nous avons pu renforcer notre offre de formation, étendre notre présence sur le marché et proposer à nos clients des programmes de certification reconnus à l'international qui font réellement la différence. L'un des résultats les plus notables de notre collaboration a été l'augmentation de la crédibilité et de la visibilité que nous avons acquises dans la région. La coordination fluide avec les équipes de PECB — en particulier en matière de diffusion des contenus et de support aux partenaires — nous a permis de servir nos clients de manière plus efficace et avec une plus grande confiance. Nous nous réjouissons de poursuivre ce partenariat solide et d'atteindre ensemble des jalons encore plus importants.

Ing. Noor Diab, MBA, Head of Strategic Advisory & Excellence Services
Aswar Akka Consultancy

Pourquoi choisir une carrière en continuité, résilience et reprise ?

- → Essentielle pour la stabilité des activités
- → Importance croissante dans tous les secteurs
- → Parcours professionnels enrichissants et à fort impact

Carrières bien rémunérées en continuité, résilience et reprise

Directeur de la gestion de crise
Responsable de la direction et de la coordination de la réponse de l'organisation aux situations d'urgence et aux situations critiques, en garantissant une planification, une préparation et des efforts de reprise efficaces.
Salaire annuel moyen : **U.S. $161,850**

Responsable de la reprise après sinistre
Spécialisé dans l'élaboration de stratégies et de plans visant à rétablir efficacement les systèmes informatiques, les données et les opérations après un sinistre. Salaire annuel moyen : **U.S. $124,920**

Responsable de la continuité des activités
Ce rôle consiste à planifier et à gérer des programmes visant à maintenir les fonctions métier ou à les reprendre rapidement en cas de perturbation majeure.
Salaire annuel moyen : **U.S. $167,985**

Chief Resilience Officer (CRO)
Le CRO est un cadre dirigeant chargé de piloter l'élaboration et la mise en œuvre de stratégies visant à gérer les risques, à se remettre des perturbations et à garantir la résilience organisationnelle.
Salaire annuel moyen : **U.S. $117,139**

Analyste / Consultant en résilience
Se concentre sur l'analyse des menaces potentielles et l'élaboration de stratégies visant à assurer la résilience organisationnelle face à divers types de perturbations.
Salaire annuel moyen : **U.S. $71,825**

Remarque : *Tes données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

PROTECTION DE LA VIE PRIVEE ET DES DONNEES

Pourquoi la protection de la vie privée et des données ?

La protection de la vie privée et des données est essentielle pour sécuriser les informations sensibles, assurer la conformité aux lois et instaurer la confiance des clients. Elles contribuent à atténuer les risques de violations et de pertes financières, soutiennent la continuité des activités et renforcent la résilience face aux cybermenaces constantes. Dans le monde numérique

ISO/IEC 27701 Privacy Information Management System

Présentation de la norme ISO/IEC 27701 et de son processus de certification

ISO/IEC 27701 est une norme internationale pour le management des informations relatives à la vie privée, fournissant des lignes directrices pour la gestion et la protection des données à caractère personnel. Le parcours de certification ISO/IEC 27701 implique une analyse approfondie des systèmes de management des informations relatives à la vie privée (PIMS). Ce processus de certification comprend l'apprentissage de la mise en place, du maintien et de l'amélioration continue d'un PIMS, aligné sur les réglementations en matière de protection des données telles que le RGPD.

Selon Global Growth Insight, le marché mondial des services de protection des données personnelles était évalué à 3,78 milliards de dollars américains en 2024 et devrait atteindre 5,33 milliards de dollars américains en 2025, pour s'élever à 74,1 milliards de dollars américains d'ici 2034, avec un TCAC de 36,08 % sur la période de prévision [2025-2034].

Avantages de la certification ISO/IEC 27701

- **Renforcement du positionnement professionnel**
- **Validation de l'expertise en management et en protection des données à caractère personnel**
- **Portée mondiale**
- **Opportunités d'évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 27701 Foundation Comprendre les concepts, principes, méthodes et techniques fondamentaux utilisés pour la mise en œuvre et le management d'un PIMS	2 JOURS
ISO/IEC 27701 Lead Implementer Acquérir la capacité de soutenir une organisation dans la planification, la mise en œuvre, le management, la surveillance et le maintien d'un PIMS basé sur la norme ISO/IEC 27701	5 JOURS
ISO/IEC 27701 Lead Auditor Développer les connaissances et les compétences nécessaires pour réaliser un audit de PIMS fondé sur les bonnes pratiques d'audit	5 JOURS
ISO/IEC 27701 Transition Comprendre les mises à jour majeures de la norme ISO/IEC 27701:2025 en apprenant comment les clauses relatives à la compréhension, à la planification et à la mise en œuvre d'un système de management des informations relatives à la vie privée (PIMS) sont désormais indépendantes et non liées à la norme ISO/IEC 27001	2 JOURS

S'inscrire

Je suis très heureux d'exprimer ma reconnaissance pour notre partenariat avec PECB. Nous apprécions particulièrement la qualité de notre collaboration ainsi que la réactivité des équipes de PECB. Les programmes de formation proposés sont également d'un excellent niveau, ce qui nous permet de garantir une offre de grande qualité à nos propres clients. Nos clients sont très satisfaits de ces formations et nous sommes ravis de poursuivre cette collaboration fructueuse avec PECB.

Eli KUDJIE
Fondateur de KEKELI ACADEMY

GDPR – Certified Data Protection Officer (CDPO)

Présentation u CDPO et de son processus de certification

La certification GDPR — Certified Data Protection Officer (CDPO) valide l'expertise en matière de législation et de pratiques de protection des données conformément au Règlement général sur la protection des données (RGPD) de l'Union européenne. L'obtention de la certification GDPR - CDPO implique une exploration approfondie des exigences du RGPD et des compétences nécessaires pour gérer efficacement la protection des données au sein d'une organisation. Ce parcours de certification comprend la compréhension du cadre juridique du RGPD, des droits des personnes concernées, des obligations des responsables du traitement et des sous-traitants, des analyses d'impact relatives à la protection des données et des protocoles de réponse aux violations de données.

Selon CMS, en 2025, l'application du RGPD demeure active et renforcée, avec plus de 5,65 milliards d'euros d'amendes infligées jusqu'en mars 2025 pour des infractions telles qu'une base juridique insuffisante pour le traitement des données et un manque de transparence. Le nombre d'amendes enregistrées est d'environ 2 245, avec une amende moyenne d'environ 2,36 millions d'euros.

Avantages de la certification CDPO

- **Maîtrise avérée du RGPD**
- **Rôle essentiel dans la protection des données**
- **Attractivité accrue sur le marché**
- **Évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
GDPR Foundation Apprendre les éléments de base pour mettre en œuvre et gérer un cadre de conformité relatif à la protection des données à caractère personnel	2 JOURS
GDPR – Certified Data Protection Officer Acquérir les compétences et les connaissances nécessaires pour piloter l'ensemble des processus de mise en œuvre d'un programme de conformité au RGPD au sein d'une organisation	5 JOURS

S'inscrire

Certified US Data Privacy

Présentation e l'USDPO et de son processus de certification

La certification Certified US Data Privacy valide une expertise avancée du paysage réglementaire et des pratiques de gouvernance qui façonnent la conformité en matière de protection des données aux États-Unis. À mesure que la législation au niveau des États se développe rapidement, les organisations ont besoin de professionnels capables d'interpréter et de mettre en œuvre les exigences des principales lois telles que le CCPA/CPRA, le VCDPA, le CPA, le CTDPA, ainsi que d'autres textes législatifs émergents au niveau des États.
La certification US Data Privacy dote les candidats des compétences nécessaires pour concevoir et gérer des programmes de protection de la vie privée conformes aux orientations fédérales et aux réglementations variées des États. Elle couvre les domaines fondamentaux de la conformité américaine en matière de protection de la vie privée, notamment les droits des consommateurs, les obligations organisationnelles, le traitement des demandes des personnes concernées, les exigences en matière d'information et de transparence, ainsi que les aspects opérationnels de la notification des violations de données et de la réponse aux incidents.
Le programme développe également des capacités stratégiques en gouvernance de la protection de la vie privée, en développement de programmes, en évaluations des risques, en gestion des fournisseurs et en coordination interfonctionnelle, des compétences essentielles pour renforcer la maturité de la protection de la vie privée au sein d'une organisation.

Avantages de la certification USDPO

- **Renforcement de la posture de conformité organisationnelle**
- **Meilleure préparation face aux nouvelles lois étatiques sur la protection de la vie privée**
- **Capacité accrue à piloter des initiatives de protection de la vie privée dès la conception (privacy-by-design)**
- **Crédibilité renforcée dans les interactions réglementaires et juridiques**
- **Meilleur alignement entre les fonctions vie privée, sécurité et gestion des risques**
- **Capacité accrue à superviser les risques liés à la protection de la vie privée des tiers**
- **Compétence améliorée dans la gestion à grande échelle des demandes des personnes concernées**
- **Opportunités de leadership élargies en gouvernance de la protection de la vie privée**
- **Confiance renforcée des clients, partenaires et parties prenantes**

Disponible bientôt

Formation et objectifs d'apprentissage	
Certified US Data Privacy Officer Développer l'expertise nécessaire pour gérer avec assurance les exigences américaines en matière de protection de la vie privée, piloter la conformité organisationnelle et soutenir des pratiques efficaces de protection des données à l'échelle de l'entreprise	5 JOURS

Disponible bientôt

Pourquoi choisir une carrière en protection de la vie privée et des données ?

- Essentielle pour la protection des informations personnelles et sensibles
- Domaine en expansion rapide en raison des avancées technologiques
- Très valorisante, avec un impact significatif sur les entreprises et la société

Carrières bien rémunérées en protection de la vie privée et des données

Chief Privacy Officer (CPO)
Rôle de cadre supérieur responsable de l'élaboration et de la mise en œuvre des politiques et pratiques de protection de protection de la vie privée, de la conformité aux lois sur la protection des données et du management des risques liés à la protection de la vie privée.
Salaire annuel moyen : **U.S. $250,000**

Privacy Counsel
Fournit une expertise juridique en matière de protection de la vie privée et des données, conseille sur la conformité aux lois sur la protection de la vie privée et gère les questions juridiques liées à la protection de la vie privée.
Salaire annuel moyen : **U.S. $215,000**

Privacy Program Manager
Gère le développement et l'exécution des programmes de protection de la vie privée, y compris les politiques, les formations et les initiatives de conformité.
Salaire annuel moyen : **U.S. $180,000**

Data Protection Officer (DPO)
Spécialisé dans la supervision de la stratégie et de la mise en œuvre de la protection des données afin d'assurer la conformité au RGPD et à d'autres lois sur la protection des données.
Salaire annuel moyen : **U.S. $145,000**

Privacy Engineer
Développe et met en œuvre des solutions techniques et des contrôles afin de garantir la confidentialité des données à caractère personnel au sein des systèmes et des applications informatiques.
Salaire annuel moyen : **U.S. $119,062**

Remarque **:** *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Chez Cynthus, nous considérons PECB comme un partenaire stratégique pour le développement des talents en Amérique latine. Son portefeuille de certifications, la mise à jour continue de ses contenus et son accompagnement académique et commercial nous permettent de concevoir des expériences d'apprentissage rigoureuses et pertinentes pour de nombreux secteurs. Grâce à PECB, nos clients renforcent leurs systèmes de management, progressent en matière de conformité et adoptent des bonnes pratiques reconnues à l'international. Je tiens également à souligner la cohérence des évaluations et la clarté des lignes directrices destinées aux centres de formation, qui garantissent une qualité de bout en bout. Nous sommes ravis d'adopter les nouveaux parcours d'apprentissage du Catalogue de formations PECB 2026 afin de continuer à créer de la valeur pour la région.

Cynthus
Mexique

IA ET TRANSFORMATION NUMÉRIQUE

Pourquoi l'intelligence artificielle ?

L'intelligence artificielle (IA) transforme les secteurs d'activité en améliorant l'efficacité et en automatisant les tâches. Elle aide les entreprises à prendre de meilleures décisions, à réduire les coûts et à obtenir un avantage concurrentiel. L'IA améliore l'expérience client et stimule l'évolution de secteurs tels que la santé, la finance et l'industrie manufacturière. En résolvant des problèmes complexes et en optimisant les opérations, l'IA constitue aujourd'hui un levier clé de réussite.

Pourquoi la transformation numérique ?

La transformation numérique est essentielle pour permettre aux entreprises de rester compétitives. Elle s'appuie sur les technologies pour optimiser les processus, améliorer l'expérience client et stimuler l'innovation. En adoptant des outils numériques, les organisations peuvent accroître leur efficacité, s'adapter aux évolutions du marché et créer de nouvelles opportunités de revenus.

ISO/IEC 42001 Artificial Intelligence Management System

Présentation de la norme ISO/IEC 42001 et de son processus de certification

La certification ISO/IEC 42001 dote les professionnels de l'expertise nécessaire pour mettre en œuvre et maintenir un système de management de l'intelligence artificielle (IA) conforme aux bonnes pratiques internationales. L'obtention de la certification ISO/IEC 42001 vous plonge dans les complexités du management de l'IA, en vous permettant d'acquérir la capacité de planifier, mettre en œuvre, gérer, surveiller, maintenir et améliorer en continu un système de management de l'intelligence artificielle (SMIA). Cette certification met également l'accent sur l'application éthique, légale et efficace de l'IA, vous préparant à jouer un rôle clé dans l'écosystème en constante évolution des technologies de l'IA.

Avantages de la certification ISO/IEC 42001 Management efficace de l'IA

- **Gestion efficace de l'IA**
- **Crédibilité renforcée**
- **Expertise spécialisée**
- **Évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 42001 Foundation Acquérir des connaissances sur les principes et concepts fondamentaux nécessaires à la mise en œuvre et au management d'un SMIA basé sur la norme ISO/IEC 42001	2 JOURS
ISO/IEC 42001 Lead Implementer Obtenir les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et le maintien d'un SMIA basé sur la norme ISO/IEC 42001	5 JOURS
ISO/IEC 42001 Lead Auditor Acquérir les connaissances et compétences nécessaires pour réaliser un audit de SMSI en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

Certified Artificial Intelligence Professional (CAIP)®

Présentation du CAIP et de son processus de certification

La formation Certified Artificial Intelligence Professional (CAIP) offre une exploration approfondie de l'intelligence artificielle en vous guidant des concepts fondamentaux aux méthodes et applications les plus avancées. Vous apprendrez à collecter et analyser des données, à concevoir et affiner des modèles d'apprentissage automatique, ainsi qu'à aborder des domaines plus avancés tels que l'apprentissage profond, le traitement du langage naturel et même la robotique. L'obtention de cette certification démontre non seulement votre expertise technique, mais met également en évidence votre engagement à concevoir des initiatives en IA sûres, conformes et créatrices de valeur pour les entreprises et la société.

Avantages de la certification Certified Artificial Intelligence Professional (CAIP)

- **Maîtrise des fondamentaux de l'IA pour des solutions innovantes**
- **Amélioration de l'analyse des données et de l'apprentissage automatique pour des décisions plus pertinentes**
- **Progression en apprentissage profond et en NLP pour une meilleure adaptabilité**
- **Prise en compte de l'éthique et de la conformité pour une utilisation responsable de l'IA**

En savoir plus

Formation et objectifs d'apprentissage

5 JOURS

Certified Artificial Intelligence Professional (CAIP)

Acquérir les connaissances et les compétences nécessaires pour explorer les concepts fondamentaux de l'IA, réaliser des analyses et des visualisations de données, concevoir et évaluer des modèles d'apprentissage automatique, et explorer les techniques de traitement du langage naturel (NLP) et d'apprentissage profond.

Dans cette formation, vous apprendrez à appliquer des cadres éthiques et réglementaires, à gérer les risques liés à l'IA et à élaborer des stratégies de gouvernance afin de garantir des déploiements d'IA responsables et efficaces.

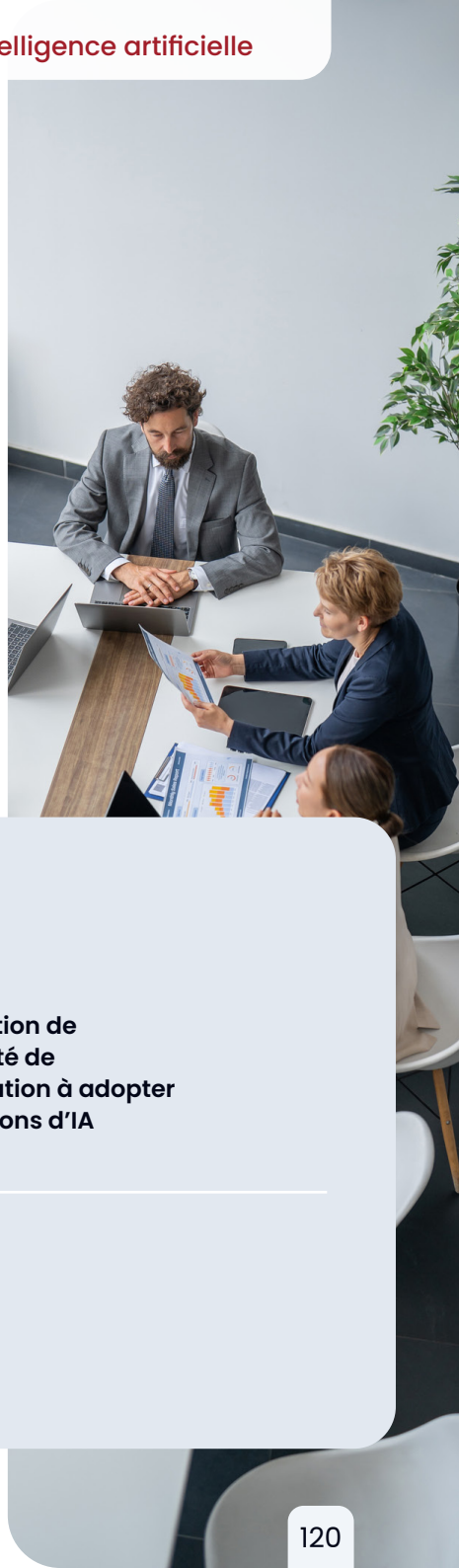
S'inscrire

AI Risk Management

Présentation de la gestion des risques liés à l'IA et de son processus de certification

La certification AI Risk Management dote les professionnels des capacités nécessaires pour superviser l'évaluation, le contrôle et le suivi des systèmes d'IA au sein de l'organisation. Elle met l'accent sur les dimensions pratiques du management des expositions liées à l'IA, allant des considérations d'équité et de transparence aux risques de sécurité et à l'intégrité opérationnelle. Les participants s'engagent dans des composantes appliquées structurées qui renforcent la capacité à identifier les risques, évaluer les impacts potentiels et mettre en place des mesures permettant d'aligner les initiatives d'IA sur les politiques internes et les exigences externes. Cette certification développe la maîtrise de l'application de cadres reconnus, notamment le NIST AI Risk Management Framework et l'EU AI Act, dans les activités quotidiennes de supervision.

Le Global Risks Report du WEF identifie la désinformation et les usages abusifs liés à l'IA parmi les risques mondiaux les plus graves à court terme, soulignant le besoin croissant d'une supervision structurée de l'IA et d'une expertise en gouvernance.



Avantages de la certification Lead AI Risk Manager

- **Compétence vérifiée en évaluation et supervision des risques liés à l'IA**
- **Renforcement de la confiance organisationnelle dans une IA responsable et conforme**
- **Amélioration de la capacité de l'organisation à adopter des solutions d'IA**
- **Amélioration de la fiabilité des performances des modèles d'IA**
- **Supervision renforcée sur l'ensemble du cycle de vie de l'IA**

En savoir plus

Formation et objectifs d’apprentissage

Lead AI Risk Manager Acquérir les connaissances essentielles pour identifier, évaluer et gérer les risques liés à l’IA, en s’appuyant sur le NIST AI RMF, l’EU AI Act et le MIT AI Risk Repository	**5 JOURS**

S’inscrire

En tant que partenaire de confiance de PECB, notre collaboration constitue un pilier de notre stratégie visant à proposer des formations de premier plan en sécurité de l'information dans la région nordique. Les formations rigoureuses de PECB, fondées sur les normes, offrent la profondeur technique et scientifique dont nous avons besoin, nous permettant de doter les professionnels de compétences concrètes pour mettre en place des SMSI résilients et gérer efficacement les risques. Ce partenariat se traduit par une valeur métier directe pour nos clients : l'atteinte de la conformité, le renforcement de la confiance des parties prenantes et l'obtention d'un avantage concurrentiel. Nous nous réjouissons à l'idée d'intégrer les nouvelles offres du Catalogue PECB 2026 afin de continuer à accompagner les organisations avec une expertise en sécurité pérenne.

Dr. Gabriel Silva
Digital2me, Costa Rica

Certified AI Manager (CAIM)®

Présentation du CAIM et de son processus de certification

La formation Certified AI Manager (CAIM) est conçue pour les dirigeants, managers et décideurs responsables de la définition de la stratégie, de la gouvernance et de la mise en œuvre de l'IA au sein de leurs organisations. Cette formation propose un parcours complet allant des concepts fondamentaux de l'IA et des tendances mondiales aux cadres pratiques pour l'identification des cas d'usage, la préparation des données, la gestion des risques et l'automatisation. Les participants étudieront des études de cas réels, apprendront à aligner les initiatives d'IA sur les objectifs métier et à comprendre les exigences réglementaires émergentes ainsi que les considérations éthiques.

Ils développeront également des compétences en prise de décision fondée sur les données à l'aide de Power BI et exploreront la conception, la gouvernance et le déploiement d'automatisations pilotées par l'IA à l'aide d'outils tels que n8n. L'obtention de cette certification démontre votre capacité à piloter des programmes d'IA de manière responsable, à traduire les capacités techniques en valeur métier et à gérer des projets d'IA sur l'ensemble de leur cycle de vie, de l'idée à l'impact.

Avantages de la certification CAIM

- **Traduire les concepts d'IA en valeur métier claire et en feuilles de route stratégiques**
- **Renforcer la gouvernance de l'IA, l'élaboration de politiques et la préparation réglementaire**
- **Améliorer la prise de décision fondée sur les données grâce à des analyses structurées et à Power BI**
- **Renforcer la capacité à identifier, prioriser et gérer des cas d'usage d'IA à fort impact**
- **Piloter des initiatives d'automatisation de l'IA responsables, conciliant innovation et gestion des**

Nouvelle formation

Formation et objectifs d'apprentissage

Certified AI Manager — 5 JOURS

CAIM dote les managers des compétences nécessaires pour concevoir et piloter des initiatives d'IA en alignant les cas d'usage sur la stratégie métier, en mettant en place une gouvernance et des contrôles des risques, et en promouvant une prise de décision responsable fondée sur les données.

Les participants acquièrent également une exposition pratique à des outils d'analytique et d'automatisation tels que Power BI et n8n afin de traduire les capacités de l'IA en valeur organisationnelle mesurable.

S'inscrire

Pourquoi choisir une carrière en intelligence artificielle (IA) ?

- → Au cœur de l'innovation et de l'automatisation
- → Moteur d'avantage concurrentiel dans tous les secteurs
- → Forte demande et excellent potentiel de rémunération

L'intelligence artificielle transforme la manière dont les organisations fonctionnent, prennent des décisions et créent de la valeur. Les professionnels de l'IA sont à l'avant-garde du développement de systèmes intelligents qui améliorent l'efficacité, la précision et l'innovation dans des secteurs tels que la finance, la santé, l'industrie manufacturière, l'assurance et la cybersécurité.

Carrières bien rémunérées en intelligence artificielle

Machine Learning Engineer
Conçoit, entraîne et optimise des modèles d'apprentissage automatique à grande échelle, en garantissant leurs performances, leur fiabilité et leur évolutivité en production.
Salaire annuel moyen : **U.S. $170,000**

AI Engineer
Conçoit, développe et déploie des modèles d'IA et d'apprentissage automatique pour résoudre des problématiques métier complexes. Ce rôle requiert de solides compétences en science des données, en algorithmes et en intégration de systèmes.
Salaire annuel moyen : **U.S. $164,000**

AI Security Engineer
Se concentre sur la sécurisation des systèmes d'IA et d'apprentissage automatique contre les attaques adversiales, l'empoisonnement des données, le vol de modèles et les usages abusifs des technologies d'IA.
Salaire annuel moyen : **U.S. $145,000 – $170,000**

Data Scientist (orienté IA)
Analyse de grands ensembles de données afin de concevoir des modèles prédictifs et prescriptifs soutenant la prise de décision pilotée par l'IA.
Salaire annuel moyen : **U.S $140,000**

Certified AI Auditor / AI Governance Specialist
Évalue les systèmes d'IA en matière de conformité, d'éthique, de transparence, de risques et d'alignement sur les exigences de gouvernance et de réglementation. Salaire annuel moyen : **U.S. $126.000**

Remarque **:** *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Certified Digital Transformation Officer (CDTO)

Présentation du CDTO et de son processus de certification

La certification Certified Digital Transformation Officer (CDTO) est une accréditation professionnelle visant à doter les individus des compétences et des connaissances nécessaires pour piloter et gérer des initiatives de transformation numérique au sein des organisations.

Le parcours de certification CDTO implique la maîtrise d'un ensemble complet de compétences essentielles pour conduire le changement numérique dans les entreprises modernes. Cette certification couvre la planification stratégique, l'adoption des technologies numériques, la gestion du changement, le développement d'une culture numérique et le leadership en matière d'innovation.

Avantages de la certification CDTO

- **Opportunités de réseautage**
- **Leadership en stratégie numérique**
- **Profil professionnel renforcé**
- **Compétences tournées vers l'avenir**

En savoir plus

Formation et objectifs d'apprentissage	
Certified Digital Transformation Officer (CDTO) Acquérir les compétences et les connaissances nécessaires pour piloter et maintenir des stratégies de transformation numérique au sein des organisations	5 JOURS

S'inscrire

Pourquoi choisir une carrière en transformation numérique ?

- → Permettre un changement à l'échelle de l'organisation
- → Aligner la technologie sur la stratégie métier
- → Forte demande aux postes de leadership et de haute direction

Les professionnels de la transformation numérique pilotent l'intégration des technologies numériques dans l'ensemble des fonctions de l'entreprise, en transformant les modèles opérationnels, les expériences clients et la culture organisationnelle. Ces rôles combinent un leadership stratégique avec une solide compréhension des technologies, de la gestion du changement et de l'innovation.

Carrières bien rémunérées en transformation numérique

Chief Digital Officer (CDO)
Cadre dirigeant responsable de la définition et de l'exécution de la stratégie numérique de l'organisation, du pilotage de l'innovation et de l'alignement entre la technologie et les objectifs métier.
Salaire annuel moyen : **U.S. $240,000**

Digital Transformation Director
Pilote les initiatives de transformation numérique entre les départements, en supervisant l'adoption des technologies, l'optimisation des processus et le changement organisationnel.
Salaire annuel moyen : **U.S. $185,000**

Enterprise Digital Architect
Conçoit des architectures numériques et technologiques à l'échelle de l'entreprise afin de soutenir les objectifs de transformation à long terme.
Salaire annuel moyen : **U.S. $155,000**

Digital Transformation Officer
Supervise l'intégration des technologies numériques dans les opérations métier, améliorant l'efficacité, l'agilité et la création de valeur pour les clients.
Salaire annuel moyen : **U.S $150,000**

Certified AI Auditor / AI Governance Specialist
Conseille les organisations en matière de stratégie numérique, de mise en œuvre technologique et de gestion du changement afin de soutenir une transformation durable.
Salaire annuel moyen : **U.S. $140,000**

Remarque **:** *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Chez Risk, Governance & Compliance Consulting, nous estimons que les formations PECB vont au-delà de la salle de classe et favorisent l'excellence professionnelle. La qualité et la profondeur des supports fournis, ainsi que la robustesse du processus de certification, garantissent que chaque participant acquiert de réelles compétences applicables aux défis actuels. Au fil des années, en tant que partenaire et formateur, j'ai pu constater comment les certifications PECB transforment la pratique et la perspective des participants, tout en renforçant leur confiance dans leur développement professionnel.

Raúl Gonzáles
Risk, Governance & Compliance Consulting, Équateur

GOUVERNANCE, RISQUE ET CONFORMITÉ

Pourquoi la gouvernance, le risque et la conformité ?

La gouvernance, le risque et la conformité (GRC) aident les organisations à atteindre leurs objectifs tout en respectant les normes éthiques, légales et réglementaires.
Elle garantit la responsabilisation, permet une gestion continue des risques et favorise une culture de conformité, réduisant les risques juridiques et renforçant la confiance des parties prenantes. La GRC permet

ISO 31000 Risk Management

Présentation de la norme ISO 31000 et de son processus de certification

La certification ISO 31000 est une norme reconnue à l'échelle mondiale qui atteste d'une expertise en principes et lignes directrices de management du risque. Le processus de certification ISO 31000 consiste à maîtriser un cadre de référence pour une gestion efficace des risques, applicable à tous les types d'organisations. Ce parcours de certification comprend la compréhension des principes, du cadre et du processus de management du risque, tels que définis dans la norme ISO 31000.

Selon Coherent Market Insights, le marché mondial du management du risque est estimé à 14,93 milliards de dollars américains en 2025 et devrait atteindre 40,20 milliards de dollars américains d'ici 2032, avec un taux de croissance annuel composé (TCAC) de 15,2 % sur la période 2025-2032.

Avantages de la certification ISO 31000

- **Renforcement des capacités professionnelles**
- **Valeur stratégique**
- **Renforcement des compétences en management du risque**
- **Évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 31000 Foundation Acquérir des connaissances sur les principaux composants de la norme ISO 31000, ses principes et ses approches en matière de management du risque	2 JOURS
ISO 31000 Risk Manager Acquérir les compétences et les connaissances nécessaires pour mettre en œuvre le processus et le cadre de management du risque au sein d'une organisation conformément aux lignes directrices définies dans la norme ISO 31000	3 JOURS
ISO 31000 Lead Risk Manager Développer les compétences nécessaires pour mettre en œuvre avec succès un processus et un cadre de management du risque basés sur la norme ISO 31000 et appliquer les principes de management du risque alignés sur la norme	5 JOURS

S'inscrire

ISO/IEC 38500 IT Governance

Présentation de la norme ISO/IEC 38500 et de son processus de certification

La certification ISO/IEC 38500 est une qualification attestant d'une expertise en gouvernance d'entreprise des technologies de l'information, fournissant des lignes directrices pour un management et une utilisation efficaces des TI au sein des organisations. Le parcours de certification ISO/IEC 38500 implique l'acquisition d'une compréhension approfondie des principes et des bonnes pratiques en matière de gouvernance des TI. Ce parcours couvre des domaines clés tels que l'établissement d'un cadre de gouvernance efficace des TI, l'alignement des TI sur les objectifs organisationnels, la garantie que les investissements informatiques sont pertinents et créateurs de valeur, ainsi que la gestion des risques et de la conformité liés aux TI.

Avantages de la certification ISO/IEC 38500

- **Gouvernance efficace des TI**
- **Influence accrue sur la stratégie informatique de l'organisation**
- **Développement professionnel**
- **Engagement envers les normes de gouvernance des TI**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 38500 Foundation Acquérir des connaissances sur les bonnes pratiques du secteur en matière de gouvernance des technologies de l'information et sur ses principes clés	**2 JOURS**
ISO/IEC 38500 IT Corporate Governance Manager Acquérir une compréhension approfondie des principes fondamentaux d'une bonne gouvernance des TI selon la norme ISO/IEC 38500 et de la mise en œuvre d'un cadre efficace	**3 JOURS**
ISO/IEC 38500 Lead IT Corporate Governance Manager Développer les compétences et les connaissances nécessaires pour évaluer, mettre en œuvre et surveiller avec succès un modèle de gouvernance des TI en suivant les lignes directrices de la norme ISO/IEC 38500	**5 JOURS**

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

ISO 37000 Corporate Governance

Présentation de la norme ISO 37000 et de son processus de certification

La norme ISO 37000 fournit des lignes directrices en matière de gouvernance d'entreprise, permettant aux organisations d'établir, de développer, d'évaluer et de maintenir des pratiques de gouvernance efficaces. La certification ISO 37000 est un titre professionnel qui valide votre expertise dans l'application des principes de gouvernance alignés sur cette norme internationale. Elle vous dote des connaissances nécessaires pour promouvoir un leadership éthique, garantir la responsabilisation et favoriser une performance durable.

En obtenant cette certification, vous démontrez votre capacité à accompagner les organisations dans l'intégration de bonnes pratiques de gouvernance dans leurs opérations, leurs processus décisionnels et leur stratégie globale, favorisant la transparence et la confiance des parties prenantes.

Avantages de la certification ISO 37000

- **Maîtrise des pratiques de gouvernance**
- **Prise de décision éthique**
- **Renforcement de la confiance des parties prenantes**
- **Opportunités de leadership**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 37000 Corporate Governance Manager Acquérir les compétences nécessaires pour aider les organisations à établir, maintenir et améliorer une bonne gouvernance basée sur la norme ISO 37000	**4 JOURS**
ISO 37000 Lead Corporate Governance Manager Acquérir les compétences nécessaires pour établir, maintenir et améliorer une bonne gouvernance au sein des organisations conformément à la norme ISO 37000	**5 JOURS**

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

ISO 37001 Anti-Bribery Management System

Présentation de la norme ISO 37001 et de son processus de certification

ISO 37001 est une norme reconnue à l'échelle mondiale qui démontre l'engagement d'une organisation à mettre en œuvre un système de management anti-corruption (SMAC) efficace. L'obtention de la certification ISO 37001 implique un processus complet de compréhension et d'application de la norme pour établir, maintenir et améliorer un SMAC. Ce parcours de certification comprend l'apprentissage des principes et pratiques liés à l'évaluation des risques de corruption, aux procédures de diligence raisonnable, aux contrôles financiers et non financiers, ainsi qu'à la mise en œuvre de politiques et de procédures visant à lutter contre la corruption.

Avantages de la certification ISO 37001

- **Compétence validée en management anti-corruption**
- **Crédibilité accrue**
- **Amélioration des opportunités professionnelles**
- **Attractivité accrue sur le marché**

En savoir plus

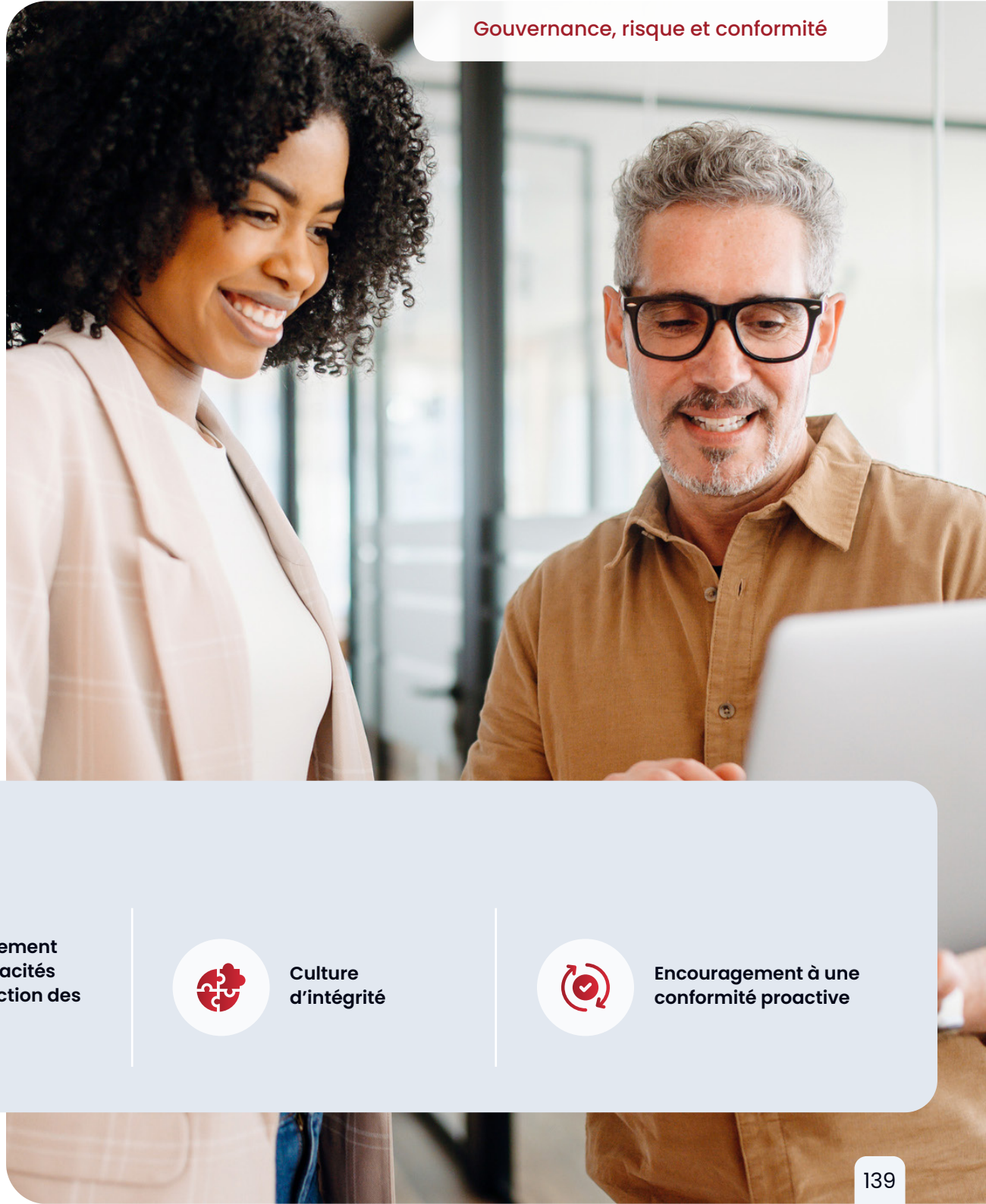
Formation et objectifs d'apprentissage	
ISO 37001 Foundation Acquérir des connaissances sur les concepts et principes d'un SMAC basé sur la norme ISO 37001 ainsi que sur la structure et les composants de la norme	2 JOURS
ISO 37001 Lead Implementer Devenir compétent pour mettre en œuvre et gérer avec succès un SMAC basé sur la norme ISO 37001	5 JOURS
ISO 37001 Lead Auditor Développer les compétences et l'expertise nécessaires pour auditer un SMAC conformément aux exigences de la norme ISO 37001 et aux autres bonnes pratiques d'audit	5 JOURS
ISO 37001:2025 Transition Comprendre les différences entre ISO 37001:201a6 et ISO 37001:2025 et acquérir les connaissances nécessaires pour aligner un SMAC sur la norme mise à jour	2 JOURS

S'inscrire

ISO 37301 Compliance Management System

Présentation de la norme ISO 37301 et de son processus de certification

ISO 37301 est une certification relative aux systèmes de management de la conformité, fournissant des lignes directrices pour aider les organisations à établir, développer, évaluer et maintenir un système de management de la conformité efficace. L'obtention de la certification ISO 37301 implique une approche systématique visant à comprendre et à mettre en œuvre les exigences de conformité au sein de votre organisation. Elle commence par une évaluation approfondie des processus de conformité existants, afin d'identifier les domaines nécessitant un alignement sur la norme ISO 37301.



Avantages de la certification ISO 37301

- **Engagement en faveur de la conformité**
- **Renforcement des capacités de réduction des risques**
- **Culture d'intégrité**
- **Encouragement à une conformité proactive**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 37301 Foundation Comprendre les concepts fondamentaux de la conformité et les exigences de la norme ISO 37301 relatives à un système de management de la conformité (SMC)	**2 JOURS**
ISO 37301 Lead Implementer Développer les compétences nécessaires à l'établissement, à la mise en œuvre, au maintien et à l'amélioration continue d'un système de management de la conformité basé sur la norme ISO 37301	**5 JOURS**
ISO 37301 Lead Auditor Acquérir les compétences et les connaissances nécessaires pour réaliser des audits de systèmes de management de la conformité basés sur la norme ISO 37301 et sur les lignes directrices pour l'audit des systèmes de management fournies dans la norme ISO 19011 ainsi que sur le processus de certification présenté dans la norme ISO/IEC 17021-1	**5 JOURS**

S'inscrire

Mon entreprise est devenue partenaire de PECB en 2014. Cette année a marqué un tournant décisif pour moi, car elle a été le point de départ d'un parcours remarquable de croissance et de développement professionnels sans précédent. Grâce à mon association avec PECB en tant que partenaire, j'ai obtenu des qualifications dans un large éventail de disciplines liées aux systèmes de management. En tant que formateur certifié PECB, j'ai formé de nombreuses personnes qui sont ensuite devenues formateurs certifiés à leur tour. Le partenariat avec PECB a représenté la meilleure opportunité pour mon entreprise. Nous sommes reconnus pour notre capacité à offrir des connaissances de pointe et à permettre aux employés, à différents niveaux, d'acquérir des compétences favorisant le développement professionnel et la création de valeur pour leurs organisations. Je recommande le partenariat avec PECB comme le meilleur choix pour toute organisation souhaitant être associée à une entreprise véritablement mondiale, guidée par des normes éthiques et fondée sur le développement mutuel.

Jacob McLean

Consultant principal et formateur en chef chez Kaizen Training and Management Consultants Limited (KTMC) – Jamaïque

Management Systems Internal Auditor

Présentation du rôle Management Systems Internal Auditor et de son processus de certification

La certification CMSIA (Certified Management Systems Internal Auditor) est une accréditation professionnelle qui valide l'expertise en management et en réalisation d'audits internes au sein des organisations. Le parcours de certification CMSIA implique l'acquisition d'une compréhension approfondie des principes et pratiques de l'audit interne. Ce processus de certification couvre des domaines clés tels que la planification et la réalisation des audits, l'évaluation des risques, les vérifications de conformité, la rédaction de rapports et les compétences en communication.

Avantages de la certification Management Systems

- **Expertise en audits internes**
- **Efficacité opérationnelle**
- **Compétences renforcées en audit**
- **Opportunités de leadership dans les domaines de l'audit et de la gouvernance**

En savoir plus

Formation et objectifs d'apprentissage

Certified Management Systems Internal Auditor

Développer les compétences nécessaires pour planifier et réaliser des audits internes de systèmes de management

3 JOURS

S'inscrire

En tant que partenaire officiel de PECB, Deming Training Center est fier de collaborer avec l'un des organismes de certification les plus reconnus au monde dans les domaines des systèmes de management ISO, de la sécurité de l'information, de la durabilité et du développement professionnel. Grâce à ce partenariat, nous avons pu offrir à nos apprenants et à nos clients entreprises des certifications reconnues à l'international, renforçant leur expertise, leur crédibilité et leur employabilité sur un marché mondial de plus en plus exigeant. Le soutien, le professionnalisme et la réactivité de l'équipe PECB sont exemplaires. La qualité des supports de formation, la rigueur des examens et l'intégrité du processus de certification correspondent parfaitement à nos valeurs. Nous nous réjouissons de poursuivre cette collaboration fructueuse avec PECB et de contribuer ensemble au développement de compétences de classe mondiale

Omar Ait Ouakha

Formateur certifié PECB et Directeur du Deming Training Center

Certified Management Systems Consultant (CMSC)

Présentation du CMSC et de son processus de certification

La certification Management Systems Consultant (CMSC) valide votre expertise en conseil et en accompagnement des organisations pour établir, optimiser et pérenniser des systèmes de management efficaces. Fondée sur des principes éprouvés, cette certification démontre votre maîtrise de méthodologies de référence et votre engagement à élever la qualité des services de conseil. Elle atteste que vous possédez l'expertise nécessaire pour guider les organisations dans la complexité de la mise en œuvre et du maintien des systèmes de management, en mettant en évidence votre capacité à fournir des solutions stratégiques et efficaces, adaptées aux besoins organisationnels.

Avantages de la certification CMSC

- **Compétences renforcées en conseil**
- **Expertise en systèmes de management**
- **Amélioration de la valeur apportée aux clients**
- **Meilleures opportunités de réseautage**

Disponible bientôt

Formation et objectifs d'apprentissage	
Management Systems Consultant Foundation Se familiariser avec les concepts théoriques et pratiques fondamentaux du conseil en systèmes de management et en acquérir la compréhension	2 JOURS
Certified Management Systems Consultant Développer les compétences et acquérir les connaissances nécessaires pour interpréter et mettre en œuvre des pratiques de conseil en systèmes de management	5 JOURS

Disponible bientôt

ISO/TS 31050 Emerging Risks

Présentation de la norme ISO/TS 31050 et de son processus de certification

ISO/TS 31050 est une norme d'orientation prospective axée sur l'identification, l'évaluation et le management des risques émergents dans un environnement mondial en évolution rapide. Le processus de certification ISO/TS 31050 dote les professionnels des connaissances et des compétences nécessaires pour anticiper les menaces futures, évaluer des risques complexes et interconnectés, et accompagner les organisations dans le renforcement de leur résilience. Cette certification implique l'apprentissage de l'application des principes liés aux risques émergents, le développement d'approches structurées de prévision des risques et l'intégration de ces pratiques dans la prise de décision organisationnelle afin de garantir la préparation dans des contextes incertains et dynamiques.

Avantages de la certification ISO/TS 31050

- **Compétence avancée en gestion des risques émergents**
- **Anticipation renforcée des menaces futures**
- **Amélioration de la résilience organisationnelle**
- **Reconnaissance en management des risques émergents**

Disponible bientôt

Formation et objectifs d'apprentissage

ISO/TS 31050 Emerging Risk Manager Acquérir les compétences nécessaires pour accompagner les organisations dans l'identification, l'analyse et la compréhension des risques émergents sur la base de la norme ISO/TS 31050	2 JOURS

Disponible bientôt

Pourquoi choisir une carrière en GRC ?

- → Domaine en évolution rapide
- → Rôles essentiels dans les entreprises modernes
- → Parcours professionnels diversifiés et à fort impact

Carrières bien rémunérées en GRC

Chief Risk Officer (CRO)
Responsable de la supervision des stratégies de management du risque de l'organisation, de l'identification des risques potentiels et de la conformité aux lois et réglementations.
Salaire annuel moyen : **U.S. $260,000**

Risk Management Director
Dirige les politiques et programmes de management du risque, en identifiant et en analysant les risques susceptibles d'avoir un impact sur l'organisation.
Salaire annuel moyen : **U.S. $170,000**

GRC Program Manager
Gère l'ensemble du programme de gouvernance, de risque et de conformité, en coordonnant les différents départements afin d'assurer l'alignement sur les objectifs stratégiques.
Salaire annuel moyen : **U.S. $150,000**

IT Governance, Risk, and Compliance Manager
Spécialisé dans la gestion des enjeux de gouvernance, de risque et de conformité liés aux technologies de l'information, y compris les risques de cybersécurité et les cadres de gouvernance des TI.
Salaire annuel moyen : **U.S. $155,000**

Compliance Officer
Supervise la fonction conformité, en veillant à ce que l'organisation respecte les exigences légales et les politiques internes.
Salaire annuel moyen : **U.S. $125,000**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Le Quality Institute du Bureau of Standards Jamaica (QI BSJ) est fier d'être partenaire de PECB depuis plusieurs années. Cette collaboration a considérablement renforcé la crédibilité et la visibilité de notre institut de formation, nous offrant un avantage concurrentiel grâce à une gamme complète de programmes de formation liés aux normes ISO. Ce partenariat a élargi notre capacité à servir les professionnels des secteurs économiques jamaïcains, renforçant ainsi notre rôle dans la promotion d'une culture de la qualité, de l'efficacité opérationnelle et de l'amélioration continue. Grâce au soutien et aux ressources de PECB, le QI BSJ est en mesure de proposer des formations de haute qualité, alignées à l'international et répondant de manière constante aux normes mondiales. Cette relation a été déterminante pour renforcer notre réputation et étendre notre portée, tant au niveau local que régional, grâce à des certifications reconnues mondialement. Le Quality Institute du Bureau of Standards Jamaica (QI BSJ) recommande vivement un partenariat avec PECB, car son accompagnement de confiance et l'étendue de ses ressources contribuent à renforcer la confiance et la satisfaction des clients. Le partenariat avec PECB permet aux organisations d'élargir leur portée sur le marché et de proposer des formations conformes à des référentiels reconnus à l'international.

Bureau of Standards Jamaica (BSJ)
Jamaïque

QUALITÉ, SANTÉ, SÉCURITÉ ET DURABILITÉ

Pourquoi la qualité et le management ?

La qualité et le management sont essentiels pour permettre aux organisations de garantir la constance, de satisfaire les clients et d'améliorer leurs opérations. Un management efficace assure une utilisation efficiente des ressources et l'atteinte des objectifs, tandis qu'un accent mis sur la qualité garantit des standards élevés. La combinaison de ces deux dimensions contribue à l'amélioration des processus, stimule l'innovation et favorise l'amélioration continue, conduisant à un avantage concurrentiel, à une meilleure réputation et à un succès durable, aligné sur les objectifs métier et les attentes des clients.

Pourquoi la santé et la sécurité ?

La santé et la sécurité sont essentielles pour protéger les employés, réduire les risques et assurer la conformité réglementaire. Une forte culture de la sécurité permet de prévenir les accidents, d'accroître la productivité et de stimuler le moral des employés.
En donnant la priorité à la santé et à la sécurité, les organisations réduisent les risques juridiques et financiers tout en améliorant leur réputation en matière de pratiques responsables et éthiques.

Pourquoi la durabilité ?

La durabilité est fondamentale pour la santé environnementale, sociale et économique à long terme. Elle contribue à réduire la consommation des ressources, à minimiser les déchets et à relever les défis climatiques, tout en améliorant l'efficacité et la réputation. Les pratiques durables stimulent l'innovation et garantissent un avenir meilleur, tant pour les entreprises que pour les communautés.

ISO 9001 Quality Management System

Présentation de la norme ISO 9001 et de son processus de certification

ISO 9001 est une norme reconnue à l'échelle internationale qui spécifie les exigences relatives à un système de management de la qualité (SMQ), en mettant l'accent sur la performance constante et la satisfaction des clients. S'engager dans le parcours de certification ISO 9001 signifie approfondir les principes du management de la qualité, applicables universellement à toute organisation, indépendamment de sa taille ou de son secteur d'activité. Ce processus de certification implique de comprendre et d'appliquer les exigences de la norme ISO 9001, notamment l'établissement d'une forte orientation client, l'engagement de la direction, l'approche processus et l'amélioration continue.

Avantages de la certification ISO 9001

- **Démontre une expertise en management de la qualité**
- **Évolution de carrière dans des fonctions de management et de direction**
- **Évolution de carrière dans des fonctions de management et de direction**
- **Carrière Flexible**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 9001 Foundation Acquérir des connaissances sur les éléments de base permettant de mettre en œuvre et de gérer un SMQ tel que défini par la norme ISO 9001, ainsi que sur les exigences de la norme	2 JOURS
ISO 9001 Lead Implementer Développer les compétences et l'expertise nécessaires pour accompagner une organisation dans la mise en œuvre, la gestion et le maintien d'un SMQ fondé sur la norme ISO 9001	5 JOURS
ISO 9001 Lead Auditor Développer les compétences et l'expertise nécessaires pour réaliser un audit ISO 9001 du SMQ d'une organisation en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

ISO 21502 Project Management

Présentation de la norme ISO 21502 et de son processus de certification

ISO 21502 est une norme qui fournit des lignes directrices pour un management de projet efficace, améliorant l'efficacité et le taux de réussite des projets dans divers secteurs. S'engager dans le parcours de certification ISO 21502 implique de maîtriser l'ensemble des principes et pratiques du management de projet tels que décrits dans la norme. Ce processus couvre un ensemble de domaines clés, notamment la planification, l'exécution, la surveillance, la maîtrise et la clôture des projets. Il met l'accent sur l'importance d'une communication efficace, de l'engagement des parties prenantes, du management des risques et de l'allocation des ressources pour gérer les projets avec succès. Le processus de certification souligne également la nécessité d'adaptabilité et de réactivité face aux changements du périmètre ou des objectifs du projet.

Avantages de la certification ISO 21502

- **Réalisation réussie des projets**
- **Démontre une expertise en management de projet**
- **Compétitivité accrue**
- **Vous dote des pratiques les plus récentes en management de projet**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 21502 Foundation Apprendre les meilleures pratiques pour le management de projet, ainsi que les concepts et processus clés qui y sont liés	2 JOURS
ISO 21502 Lead Project Manager Acquérir l'expertise nécessaire pour diriger une organisation et son équipe afin de mettre en œuvre, gérer et maintenir des projets fondés sur la norme ISO 21502	5 JOURS

S'inscrire

Depuis 2010, Behaviour Brasil est fière d'être le représentant pionnier de PECB au Brésil. Au fil des années, nous avons certifié un grand nombre de professionnels devenus des références dans leurs secteurs respectifs, contribuant à l'avancement de l'excellence en management organisationnel dans tout le pays. Notre partenariat avec PECB repose sur la confiance, l'éthique et un engagement commun envers la qualité. Behaviour Brasil s'est positionnée comme le principal partenaire de PECB au Brésil, en offrant le portefeuille le plus complet de formations ISO. Cette réussite est le résultat direct de la capacité remarquable de PECB à maintenir un référentiel complet et actualisé des normes relatives aux systèmes de management ISO. PECB se distingue comme une organisation éthique, responsable et engagée, profondément attachée à ses partenaires, aux professionnels certifiés et aux organisations qu'elle sert. Les professionnels et les entreprises titulaires de certifications PECB sont très appréciés sur le marché, bénéficiant de la crédibilité d'un organisme de certification reconnu et accrédité à l'échelle internationale. Nous sommes convaincus que notre partenariat avec PECB continuera à produire un impact significatif et durable sur le développement professionnel et organisationnel à travers l'Amérique latine.

Fábio Anjos and Luciane Oliveira

PDG et responsables de la formation et du développement chez Behaviour Brasil

ISO 28000 Supply Chain Security Management System

Présentation de la norme ISO 28000 et de son processus de certification

ISO 28000 est une norme internationale relative aux systèmes de management de la sécurité de la chaîne d'approvisionnement, conçue pour renforcer les processus de sécurité et atténuer les risques au sein des chaînes d'approvisionnement. S'engager dans le parcours de certification ISO 28000 implique d'acquérir une compréhension approfondie des principes du management de la sécurité de la chaîne d'approvisionnement. Ce processus de certification comprend l'apprentissage de la mise en œuvre et de la gestion d'un système de sécurité traitant les menaces potentielles à différents stades de la chaîne d'approvisionnement. Les principaux éléments de la certification incluent l'évaluation des risques, l'élaboration de politiques de sécurité, la planification et la mise en œuvre de mesures de sécurité, ainsi que des protocoles de réponse aux situations d'urgence.

Avantages de la certification ISO 28000

- **Reconnaissance sectorielle en sécurité de la chaîne approvisionnement et en management des risques**
- **Efficacité opérationnelle de la chaîne approvisionnement**
- **Opportunités internationales**
- **Potentiel accru d'accès à des fonctions de direction**

En savoir plus

Formation et objectifs d'apprentissage

ISO 28000 Foundation Apprendre les bonnes pratiques contribuant à la mise en œuvre d'un système de management de la sécurité de la chaîne d'approvisionnement conformément aux exigences de la norme ISO 28000	2 JOURS
ISO 28000 Lead Implementer Acquérir les connaissances et compétences nécessaires pour accompagner une organisation dans l'établissement, la mise en œuvre et la gestion d'un système de management de la sécurité de la chaîne d'approvisionnement	5 JOURS
ISO 28000 Lead Auditor Développer les compétences et connaissances nécessaires pour réaliser des audits de SMSCA conformément aux exigences de la norme ISO 28000	5 JOURS
ISO 28000:2022 Transition Comprendre les différences entre ISO 28000:2007 et ISO 28000:2022 et acquérir des connaissances sur les nouveaux concepts, exigences et recommandations	5 JOURS

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

ISO 13485 Medical Devices Quality Management System

Présentation de la norme ISO 13485 et de son processus de certification

La certification ISO 13485 est une norme spécialisée qui démontre la conformité aux systèmes de management de la qualité pour la conception et la fabrication des dispositifs médicaux. Le parcours vers l'obtention de la certification ISO 13485 implique l'acquisition d'une compréhension approfondie des exigences d'un système de management de la qualité complet propre à l'industrie des dispositifs médicaux. Ce processus de certification comprend l'apprentissage des exigences relatives à la conception, au développement, à la production et à la fourniture de dispositifs médicaux qui répondent de manière constante aux exigences des clients et aux exigences réglementaires.

Avantages de la certification ISO 13485

- **Avantage sur le marché de l'emploi**
- **Crédibilité accrue dans la conception de dispositifs médicaux**
- **Valide l'expertise dans l'industrie des dispositifs médicaux**
- **Évolution de carrière**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 13485 Foundation Acquérir des connaissances sur les bonnes pratiques du secteur pour la mise en œuvre d'un SMQDM fondé sur la norme ISO 13485	2 JOURS
ISO 13485 Lead Implementer Développer les compétences nécessaires pour accompagner une organisation dans la mise en œuvre, la gestion et le maintien d'un SMQDM fondé sur la norme ISO 13485	5 JOURS
ISO 13485 Lead Auditor Développer les compétences nécessaires pour réaliser un audit de SMQDM en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

Note: *The update of the training courses has been discontinued for the time being.*

ISO/IEC 17025 Laboratory Management System

Overview of ISO/IEC 17025 and Its Certification Process

ISO/IEC 17025 is an international standard that specifies the general requirements for the competence, impartiality, and consistent operation of laboratories. Embarking on the ISO/IEC 17025 certification process involves a deep understanding of laboratory operations and the ability to implement a quality management system. This certification covers critical areas such as technical competence, equipment calibration, testing methodologies, quality control, and reporting accuracy.

According to Imarc, the global calibration services market is expected to grow from U.S. $6.2 billion in 2024 to U.S. $9.2 billion by 2033 — underscoring the growing importance of accredited testing and calibration laboratories.

Benefits of ISO/IEC 17025 Certification

- **Business Opportunities**
- **Enhanced Expertise in Managing a Laboratory**
- **Increased Trust**
- **Enhanced Credibility**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 17025 Foundation Acquérir des connaissances sur les principaux éléments permettant de mettre en œuvre un SML tel que défini dans la norme ISO/IEC 17025	2 JOURS
ISO/IEC 17025 Lead Implementer Développer les compétences et connaissances nécessaires pour accompagner un laboratoire dans la mise en œuvre, la gestion et le maintien réussis d'un SML fondé sur les exigences de la norme ISO/IEC 17025	5 JOURS
ISO/IEC 17025 Lead Assessor Acquérir une expertise en techniques d'évaluation et diriger un audit de certification ISO/IEC 17025	5 JOURS

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

Alcodefi est très satisfaite du partenariat établi avec PECB. Les formations certifiantes que nous proposons dans le cadre de cette collaboration répondent pleinement aux attentes de nos clients et améliorent la qualité de notre offre. Elles apportent une réelle valeur ajoutée en termes de reconnaissance internationale, de développement professionnel et de perfectionnement des compétences des participants. Nous nous réjouissons de poursuivre cette collaboration fructueuse.

Salem Tigzirine
Directeur général chez ALCODEFI

ISO/IEC 20000 IT Service Management System

Présentation de la norme ISO/IEC 20000 et de son processus de certification

ISO/IEC 20000 est une norme internationale qui démontre l'excellence et atteste des bonnes pratiques en management de services des TI. L'obtention de la certification ISO/IEC 20000 implique une compréhension approfondie et la conformité aux exigences du management de services des TI (SMSTI). Ce parcours comprend la maîtrise des principes de conception, de mise en œuvre, d'exploitation, de surveillance et d'amélioration d'un système de SMSTI. Vous apprendrez à aligner les services informatiques sur les besoins de l'entreprise, à gérer et fournir les services efficacement, et à améliorer en continu la qualité des services.

Selon Grand View Research, la taille du marché mondial des services informatiques était estimée à 1,50 trillion de dollars américains en 2024 et devrait atteindre 2,59 trillions de dollars américains d'ici 2030, avec un TCAC de 9,4 % entre 2025 et 2030

Avantages de la certification ISO/IEC 20000

- **Aligne les services informatiques sur les objectifs de l'entreprise**
- **Valide la capacité à gérer les services informatiques**
- **Améliorations opérationnelles**
- **Potentiel de rémunération plus élevé**

En savoir plus

Formation et objectifs d'apprentissage	
ISO/IEC 20000 Foundation Acquérir des connaissances sur les principes et processus de mise en œuvre d'un SMSTI	2 JOURS
ISO/IEC 20000 Lead Implementer Développer les compétences et l'expertise nécessaires pour mettre en œuvre et gérer un SMSTI fondé sur la norme ISO/IEC 20000	5 JOURS
ISO/IEC 20000 Lead Auditor Développer les compétences et acquérir les connaissances nécessaires pour planifier et réaliser des audits de SMSTI conformément aux exigences de la norme ISO/IEC 20000	5 JOURS

S'inscrire

S'associer à PECB a renforcé notre crédibilité et élargi notre présence mondiale en management ISO et en audit de la sécurité de l'information. Grâce à cette collaboration, nous avons obtenu l'accès à des programmes de certification de classe mondiale, à des méthodologies d'audit cohérentes et à un cadre fiable qui élève la qualité de nos services. L'expertise de PECB nous a aidés à fournir des solutions de conformité et de gouvernance à valeur ajoutée, reconnues à l'échelle mondiale. Nous recommandons vivement PECB pour son intégrité, son professionnalisme et son engagement envers l'excellence. Son écosystème de certification reconnu à l'échelle mondiale permet aux organisations de se développer avec confiance et crédibilité. S'associer à PECB signifie rejoindre une communauté qui définit et fait progresser les bonnes pratiques en matière d'audit, de management des risques et de conformité

ISMPP
États-Unis

Six Sigma Belts

Présentation des Six Sigma Belts et de leur processus de certification

La certification Six Sigma est une certification en management de la qualité qui valide l'expertise dans l'identification et l'élimination des défauts ou des inefficacités dans les processus métier à l'aide de méthodes statistiques. S'engager dans un parcours de certification Six Sigma signifie approfondir une approche systématique d'amélioration des processus par la résolution de problèmes et l'analyse statistique. La certification comprend généralement différents niveaux de ceinture – Yellow, Green, Black et Master Black – chacun représentant un niveau plus approfondi de compréhension et d'application pratique de la méthodologie Six Sigma.

Avantages de la certification Six Sigma

- **Améliore les compétences professionnelles**
- **Renforce l'attractivité sur le marché de l'emploi**
- **Démontre une expertise en amélioration des processus**
- **Augmente la valeur intersectorielle**

En savoir plus

Formation et objectifs d’apprentissage

Six SIGMA Green Belt Développer les connaissances techniques et les compétences nécessaires pour améliorer les processus dans un contexte organisationnel	**5 JOURS**

S’inscrire

ISO 21001 Educational Organizations Management System

Présentation de la norme ISO 21001 et de son processus de certification

ISO 21001 est une norme internationale axée sur les systèmes de management des organismes d'éducation (SMOE), fournissant des exigences et des lignes directrices pour la prestation et l'amélioration des services éducatifs. L'obtention de la certification ISO 21001 implique une compréhension approfondie du SMOE en apprenant à appliquer efficacement les exigences de la norme afin d'améliorer la qualité de l'éducation et d'aligner les services éducatifs sur les besoins des apprenants. Elle couvre des domaines tels que l'élaboration des programmes, les méthodes d'enseignement, les processus d'évaluation et la gestion des ressources pédagogiques.

Avantages de la certification ISO 21001

- **Amélioration de la qualité de l'éducation**
- **Satisfaction accrue des apprenants**
- **Opportunités de leadership en management de l'éducation**
- **Renforcement de la réputation des éducateurs et des établissements**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 21001 Foundation Apprendre les principaux concepts et principes d'un SMOE fondé sur la norme ISO 21001	2 JOURS
ISO 21001 Lead Implementer Développer les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un SMOE fondé sur la norme ISO 21001	5 JOURS
ISO 21001 Lead Auditor Acquérir les compétences et connaissances nécessaires pour réaliser un audit ISO 21001 en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

ISO 55001 Asset Management System

Présentation de la norme ISO 55001 et de son processus de certification

ISO 55001 est une norme internationale relative aux systèmes de management des actifs, qui spécifie les exigences pour la gestion efficace des actifs tout au long de leur cycle de vie. L'obtention d'une certification ISO 55001 implique d'acquérir une compréhension approfondie des principes et pratiques du management des actifs. Ce processus de certification comprend l'apprentissage de l'élaboration, de la mise en œuvre, du maintien et de l'amélioration d'un système de management des actifs (SMA), en veillant à ce que les actifs soient gérés et utilisés de la manière la plus efficace possible.

Avantages de la certification ISO 55001

- **Validation de l'expertise en management efficace des actifs**
- **Opportunités d'évolution de carrière**
- **Capacités renforcées d'utilisation des actifs**
- **Reconnaissance internationale des compétences ISO 55001**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 55001 Foundation Comprendre les principaux concepts et éléments nécessaires pour mettre en œuvre et gérer un système de management des actifs conformément à la norme ISO 55001	2 JOURS
ISO 55001 Lead Implementer Développer les compétences et connaissances requises pour accompagner une organisation dans la mise en œuvre, la gestion et l'amélioration d'un système de management des actifs (SMA) fondé sur les exigences de la norme ISO 55001	5 JOURS
ISO 55001 Lead Auditor Acquérir les compétences nécessaires pour réaliser des audits de SMA conformément aux exigences de la norme ISO 55001 et gérer une équipe d'auditeurs	5 JOURS
ISO 55001:2024 Transition Comprendre les différences entre ISO 55001:2014 et ISO 55001:2024 et acquérir des connaissances sur les concepts, exigences et recommandations mis à jour	2 JOURS

S'inscrire

Pourquoi choisir une carrière en qualité et management ?

- → Essentiel pour garantir des normes élevées et l'efficacité
- → Clé de l'amélioration continue dans les organisations
- → Parcours professionnel offrant des opportunités diversifiées et des avantages financiers

Carrières bien rémunérées en qualité et management

Directeur du management de la qualité
Supervise les systèmes, politiques et procédures de management de la qualité, en veillant à la conformité aux normes et réglementations du secteur.
Salaire annuel moyen : **U.S. $174,824**

Responsable de la qualité des données
Garantit que les données sont exactes, cohérentes et fiables au sein de l'organisation en mettant en œuvre des normes de qualité des données et des pratiques de gouvernance favorisant la conformité et une prise de décision éclairée.
Salaire annuel moyen : **U.S. $139,122**

Responsable assurance qualité
Gère et coordonne les activités d'assurance qualité, en mettant l'accent sur le maintien de la qualité des produits ou des services. Salaire annuel moyen : **U.S. $132,294**

Responsable qualité
Responsable de l'élaboration, de la mise en œuvre et de la supervision des systèmes qualité et des initiatives d'amélioration continue.
Salaire annuel moyen : **U.S. $125,434**

Responsable du contrôle qualité
Dirige les inspections, essais et procédures de contrôle qualité afin de garantir que les produits répondent aux spécifications requises.
Salaire annuel moyen : **U.S. $107,132**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

S'associer à PECB a été une expérience extrêmement positive et enrichissante pour Nash Partner Training Ltd. L'équipe PECB est constamment disponible, réactive et professionnelle, rendant la collaboration à la fois fluide et productive. Le vaste catalogue de formations mondialement reconnues de PECB nous a permis d'offrir à nos clients des formations hautement pertinentes pour l'environnement commercial actuel et les besoins de développement professionnel individuel. Ces programmes ont renforcé notre capacité à proposer des formations de haute qualité, accréditées à l'échelle internationale, dans les Caraïbes et en Amérique latine. Nous recommandons vivement de s'associer à PECB à toute organisation recherchant un prestataire fiable de solutions de formation de haute qualité incarnant la qualité, l'intégrité et l'amélioration continue.

Nash Partner Training Ltd
Jamaïque

ISO 45001 Occupational Health and Safety Management System

Présentation de la norme ISO 45001 et de son processus de certification

ISO 45001 est une norme internationale qui fournit un cadre pour un système de management de la santé et de la sécurité au travail efficace. S'engager dans le parcours de certification ISO 45001 implique de maîtriser les principes du management de la santé et de la sécurité au travail. Ce processus comprend une évaluation complète des dangers sur le lieu de travail, la mise en œuvre de stratégies efficaces d'atténuation des risques et la promotion d'un environnement de travail sûr et sain. La certification met l'accent sur la gestion proactive des risques en matière de santé et de sécurité, la formation des employés et l'amélioration continue des pratiques de sécurité.

Selon l'Organisation internationale du Travail, 361 milliards de dollars américains pourraient être économisés à l'échelle mondiale grâce à la mise en œuvre de mesures améliorées en matière de santé et de sécurité pour prévenir les blessures liées à la chaleur excessive sur le lieu de travail

Avantages de la certification ISO 45001

- **Augmente la valeur professionnelle**
- **Renforce la capacité à gérer un SMSST**
- **Ouvre des opportunités d'évolution de carrière**
- **Valide l'expertise**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 45001 Foundation Apprendre les principales étapes et les éléments nécessaires pour mettre en œuvre et gérer un SMSST fondé sur la norme ISO 45001	2 JOURS
ISO 45001 Lead Implementer Développer les compétences et connaissances nécessaires pour mettre en œuvre, gérer et maintenir un SMSST fondé sur la norme ISO 45001	5 JOURS
ISO 45001 Lead Auditor Développer les compétences nécessaires pour réaliser des audits de SMSST en appliquant des principes, procédures et méthodes d'audit largement reconnus	5 JOURS

S'inscrire

ISO 22000 Food Safety Management System

Présentation de la norme ISO 22000 et de son processus de certification

ISO 22000 est une norme internationale qui spécifie les exigences relatives à un système de management de la sécurité des denrées alimentaires (SMSDA), garantissant la production et les chaînes d'approvisionnement alimentaires sûres. S'engager dans la certification ISO 22000 implique un parcours complet à travers les principes du management de la sécurité des denrées alimentaires. Ce processus de certification comprend la compréhension et la mise en œuvre d'éléments critiques tels que l'analyse des dangers, les programmes prérequis opérationnels (PRPo), les points critiques pour la maîtrise (HACCP) et des politiques efficaces de sécurité des denrées alimentaires.

Avantages de la certification ISO 22000

- **Compétence démontrée en management des risques liés à la sécurité des denrées alimentaires**
- **Renforcement de la réputation professionnelle**
- **Engagement envers la qualité**
- **Attractivité auprès des employeurs**

En savoir plus

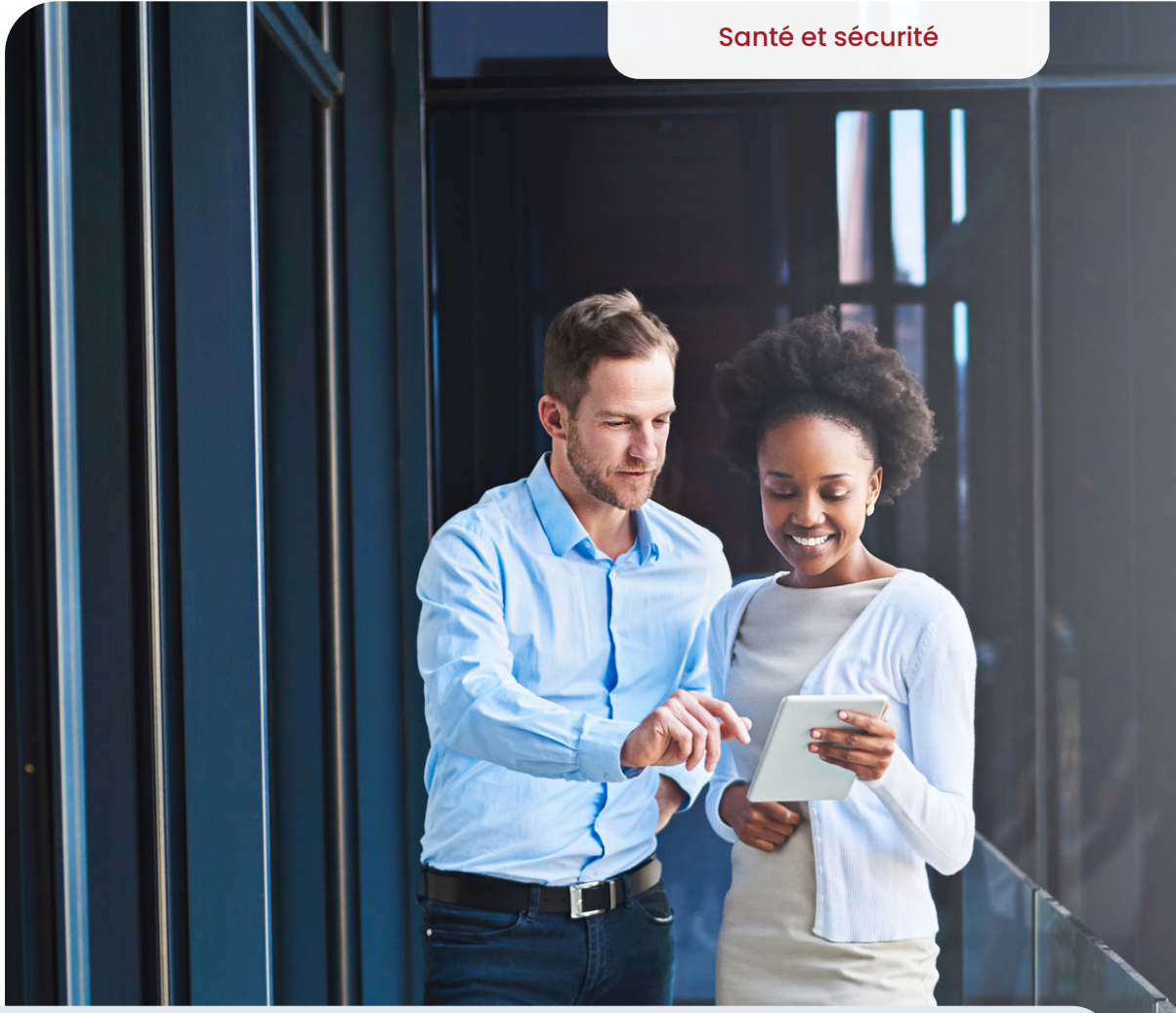
Formation et objectifs d'apprentissage	
ISO 22000 Foundation Acquérir des connaissances sur les principaux éléments et les pratiques clés du secteur pour la mise en œuvre d'un SMSDA fondé sur la norme ISO 22000	2 JOURS
ISO 22000 Lead Implementer Développer les compétences et connaissances nécessaires pour mettre en œuvre, gérer et maintenir avec succès un SMSDA fondé sur les exigences de la norme ISO 22000	5 JOURS
ISO 22000 Lead Auditor Maîtriser les techniques d'audit afin de réaliser avec succès des audits de SMSDA conformément aux exigences de la norme ISO 22000	5 JOURS

S'inscrire

ISO 18788 Security Operations Management System

Présentation de la norme ISO 18788 et de son processus de certification

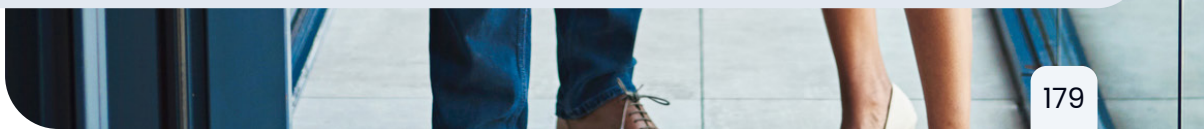
La certification ISO 18788 fournit un cadre pour établir, mettre en œuvre, exploiter, surveiller, revoir et améliorer le management des opérations de sécurité. S'engager dans le parcours de certification ISO 18788 implique d'acquérir une compréhension approfondie du système de management des opérations de sécurité privée. Ce processus de certification comprend l'apprentissage de l'élaboration et de la mise en œuvre de politiques et procédures alignées sur la protection des droits de l'homme, garantissant des pratiques commerciales éthiques et de qualité, et soutenant la cohérence des opérations de sécurité.



Avantages de la certification ISO 18788

- **Connaissances renforcées pour les opérations de sécurité privée**
- **Crédibilité professionnelle**
- **Respect des normes**
- **Valide la capacité à gérer des opérations de sécurité**

En savoir plus



Formation et objectifs d'apprentissage	
ISO 18788 Foundation Se familiariser avec les fondamentaux d'un SMOS et les meilleures pratiques pour le mettre en œuvre et le gérer, conformément à la norme ISO 18788	2 JOURS
ISO 18788 Lead Implementer Développer les compétences et connaissances nécessaires pour accompagner une organisation dans la mise en œuvre, la gestion et le maintien d'un SMOS fondé sur la norme ISO 18788	5 JOURS
ISO 18788 Lead Auditor Développer les compétences nécessaires pour réaliser un audit de SMOS en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

Pourquoi choisir une carrière en santé et sécurité ?

- Essentiel pour garantir la sécurité au travail et le respect des normes de santé
- Primordial pour prévenir les blessures et les risques professionnels
- Profession offrant un impact valorisant et des avantages financiers

Carrières bien rémunérées en santé et sécurité

Directeur environnement, santé et sécurité
Dirige la planification stratégique et la mise en œuvre des politiques de santé et de sécurité afin de garantir un environnement de travail sûr. Salaire annuel moyen : **U.S. $140,000**

Chief Safety Officer (CSO)
Responsable de la supervision des politiques et programmes globaux de sécurité au sein d'une organisation.
Salaire annuel moyen : **U.S. $150,000**

Responsable santé et sécurité
Gère et coordonne les programmes de santé et de sécurité, en veillant à la conformité aux lois et réglementations.
Salaire annuel moyen : **U.S. $100,000**

Responsable environnement, santé et sécurité (EHS Manager)
Supervise les programmes visant à garantir la conformité environnementale, sanitaire et sécuritaire sur le lieu de travail.
Salaire annuel moyen : **U.S. $108,000**

Spécialiste en santé et sécurité au travail
Se concentre sur l'identification et l'atténuation des dangers sur le lieu de travail, la conduite de formations en sécurité et la garantie de la conformité réglementaire.
Salaire annuel moyen : **U.S. $85,000**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

S'associer à PECB a été une excellente collaboration. Le partenariat PECB/Arrakis a élargi la présence de notre entreprise vers de nouvelles orientations internationales, tout en attirant de nouveaux participants aux formations au sein de l'écosystème PECB. De plus, Arrakis étant principalement un cabinet de conseil disposant d'une division formation et de nombreux services managés, la possibilité de se référer directement aux formations PECB et à une documentation ISO valide comme documents de référence sous-jacents soutient fortement notre processus de conseil. En résumé, s'associer à PECB en vaut largement la peine ; vous ne regretterez pas le professionnalisme et le soutien qu'ils offrent.

Arrakis Consulting
États-Unis

ISO 50001 Energy Management System

Présentation de la norme ISO 50001 et de son processus de certification

ISO 50001 est une norme internationale qui spécifie les exigences relatives à l'établissement, la mise en œuvre, le maintien et l'amélioration d'un système de management de l'énergie. S'engager dans le parcours de certification ISO 50001 implique de maîtriser un cadre pour un management efficace de l'énergie au sein des organisations. Ce processus comprend la compréhension des principes du management de l'énergie, notamment l'élaboration d'une politique énergétique, la définition d'objectifs énergétiques atteignables et la conception de plans d'action pour atteindre ces objectifs.

Avantages de la certification ISO 50001

- **Amélioration de l'efficacité énergétique**
- **Valeur professionnelle accrue**
- **Assurance de conformité**
- **Réduction des coûts**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 50001 Foundation Apprendre les principaux éléments nécessaires pour mettre en œuvre et gérer un SMÉ	2 JOURS
ISO 50001 Lead Implementer Acquérir les compétences et connaissances nécessaires pour accompagner une organisation dans l'établissement, la mise en œuvre, la gestion et le maintien d'un SMÉ	5 JOURS
ISO 50001 Lead Auditor Acquérir les connaissances et compétences nécessaires pour planifier et réaliser des audits de SMÉ en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

ISO 14001 Environmental Management System

Présentation de la norme ISO 14001 et de son processus de certification

ISO 14001 est une norme reconnue à l'échelle internationale relative aux systèmes de management environnemental (SME), axée sur les pratiques durables et la réduction de l'impact environnemental. S'engager dans le parcours de certification ISO 14001 implique une compréhension approfondie des systèmes de management environnemental et de leur mise en œuvre. Ce processus comprend l'apprentissage de l'élaboration, du maintien et de l'amélioration continue d'un SME, en veillant à ce qu'il gère efficacement les aspects et impacts environnementaux associés aux activités de l'organisation.

Avantages de la certification ISO 14001

- **Engagement en faveur de la durabilité**
- **Crédibilité professionnelle en matière de gestion environnementale**
- **Avantage concurrentiel**
- **Capacité démontrée à gérer la performance environnementale**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 14001 Foundation Acquérir des connaissances sur les principaux éléments permettant de mettre en œuvre et de gérer un SME tel que spécifié dans la norme ISO 14001	2 JOURS
ISO 14001 Lead Implementer Acquérir les connaissances nécessaires pour accompagner une organisation dans la mise en œuvre, la gestion et le maintien d'un SME tel que spécifié dans ISO 14001	5 JOURS
ISO 14001 Lead Auditor Développer les compétences nécessaires pour réaliser un audit de SMOS en appliquant des principes, procédures et techniques d'audit largement reconnus	5 JOURS

S'inscrire

IGP Perú et PECB : Unis pour l'excellence mondiale. Chez IGP Perú, nous nous engageons à stimuler la croissance de nos clients grâce à des formations à fort impact qui renforcent leur développement professionnel et organisationnel. Notre partenariat avec PECB renforce cette mission en combinant leur expertise en certification reconnue à l'échelle internationale avec notre expérience en formation afin de proposer des programmes qui améliorent les talents, la compétitivité et les normes de management. Ensemble, nous œuvrons pour offrir une formation de classe mondiale qui inspire, transforme et contribue au progrès durable des organisations.

IGP
Perú

ISO 26000 Social Responsibility Management System

Présentation de la norme ISO 26000 et de son processus de certification

La norme ISO 26000 est une ligne directrice relative à la responsabilité sociétale qui aide les organisations à fonctionner de manière éthique et transparente, contribuant ainsi à la santé et au bien-être de la société. S'engager dans le parcours de certification ISO 26000 implique de comprendre et d'intégrer la responsabilité sociétale dans les valeurs et les pratiques d'une organisation. Ce processus comprend l'apprentissage des principes de la responsabilité sociétale, tels que le comportement éthique, la transparence, le respect des intérêts des parties prenantes et la durabilité environnementale.

Avantages de la certification ISO 26000

- **Renforce l'expertise en RSE**
- **Soutient les objectifs de durabilité**
- **Engagement des parties prenantes**
- **Capacité renforcée en matière d'orientation vers des pratiques éthiques**

En savoir plus

Formation et objectifs d'apprentissage	
ISO 26000 Foundation Apprendre les meilleures pratiques pour orienter les organisations vers un fonctionnement socialement responsable	**2 JOURS**
ISO 26000 Lead Manager Acquérir des connaissances et compétences complètes dans le domaine de la responsabilité sociétale, conformément aux indications de la norme ISO 26000	**5 JOURS**

S'inscrire

Grâce au partenariat avec PECB, SMATICA a pu proposer à ses clients des formations et certifications de classe mondiale bénéficiant d'une reconnaissance internationale. PECB est désormais un nom de référence parmi les organismes de certification de personnes, reconnu tant par les clients du secteur public que privé lorsqu'ils souhaitent faire certifier leurs employés selon les normes ISO et les technologies les plus récentes. PECB propose un programme de revendeur attractif, avec un parcours de reconnaissance vers la réussite pour les prestataires de formation.

SMATICA LLC
États-Unis

ISO 20400 Guidelines for Sustainable Procurement

Présentation de la norme ISO 20400 et de son processus de certification

ISO 20400 est une norme relative aux achats durables, guidant les organisations dans la mise en œuvre de processus d'achat socialement, économiquement et environnementalement durables. S'engager dans le parcours de certification ISO 20400 implique d'acquérir une compréhension approfondie des principes et pratiques des achats durables. Ce processus couvre les stratégies d'intégration de la durabilité dans les politiques d'achat, les processus décisionnels et l'ensemble de la chaîne d'approvisionnement.

Avantages de la certification ISO 20400

- **Expertise en achats durables**
- **Capacité décisionnelle**
- **Crédibilité professionnelle**
- **Contribue à la durabilité organisationnelle**

En savoir plus

Formation et objectifs d'apprentissage

ISO 20400 Lead Manager

Aider les organisations à intégrer la durabilité dans leurs politiques et pratiques d'achat

5 JOURS

S'inscrire

Remarque : *La mise à jour des formations a été interrompue pour le moment.*

ISO 56001 Innovation Management System

Présentation de la norme ISO 56001 et de son processus de certification

ISO 56001 est une norme internationale qui fournit des exigences et des lignes directrices pour l'établissement, la mise en œuvre, le maintien et l'amélioration continue d'un système de management de l'innovation (SMI). Le processus de certification dote les professionnels des connaissances et compétences nécessaires pour stimuler une innovation structurée, soutenir la créativité organisationnelle et garantir une création de valeur durable. Cette certification comprend l'apprentissage de l'application des principes du management de l'innovation, du développement des processus d'innovation et de l'intégration des pratiques d'innovation dans les activités stratégiques et opérationnelles d'une organisation.

Benefits of ISO 56001 Certification

- **Capacité d'innovation structurée**
- **Créativité organisationnelle renforcée**
- **Amélioration de la gouvernance de l'innovation**
- **Renforcement des processus de création de valeur**

Disponible bientôt

Training Course and Learning Objectives	
ISO 56001 Foundation Comprendre les concepts, principes, méthodes et techniques fondamentaux utilisés pour la mise en œuvre et la gestion d'un système de management de l'innovation (SMI)	2 JOURS
ISO 56001 Lead Implementer Acquérir la capacité d'accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et le maintien d'un système de management de l'innovation (SMI) fondé sur la norme ISO 56001	5 JOURS
ISO 56001 Lead Auditor Développer les connaissances et compétences nécessaires pour réaliser un audit de certification ISO 56001 fondé sur les bonnes pratiques et méthodologies d'audit	5 JOURS

Disponible bientôt

Pourquoi choisir une carrière en durabilité ?

- → Essentielle pour relever les défis environnementaux
- → Demande croissante dans divers secteurs
- → Offre des opportunités d'avoir un impact positif sur la planète et la société

Carrières bien rémunérées en durabilité

Chief Sustainability Officer (CSO)
Poste de haute direction responsable de l'intégration de pratiques écologiques dans la stratégie et les opérations d'une organisation.
Salaire annuel moyen : **U.S. $170,000**

Directeur du développement durable
Supervise et met en œuvre les initiatives et programmes de durabilité au sein d'une organisation.
Salaire annuel moyen : **U.S. $150,000**

Responsable de programme environnemental
Gère les programmes environnementaux en mettant l'accent sur les objectifs de durabilité et l'impact environnemental.
Salaire annuel moyen : **U.S. $115,000**

Consultant en développement durable
Conseille les entreprises sur l'élaboration et la mise en œuvre de stratégies en matière de pratiques durables.
Salaire annuel moyen : **U.S. $92,000**

Analyste en développement durable
Analyse et rend compte de la performance en matière de durabilité d'une organisation et élabore des stratégies pour l'améliorer.
Salaire annuel moyen : **U.S. $70,000**

Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

Le nouveau catalogue des services de formation et de certification reflète clairement une compréhension des tendances du marché et des besoins évolutifs des organisations. Son accent mis sur le développement des compétences et l'accréditation des aptitudes apporte une valeur significative, garantissant des professionnels hautement qualifiés, compétents et alignés sur les exigences actuelles du monde du travail.

César Augusto Duque
PDG chez CIRECOM, République dominicaine

*my*PECB – À la tête d'une nouvelle ère d'expériences numériques personnalisées

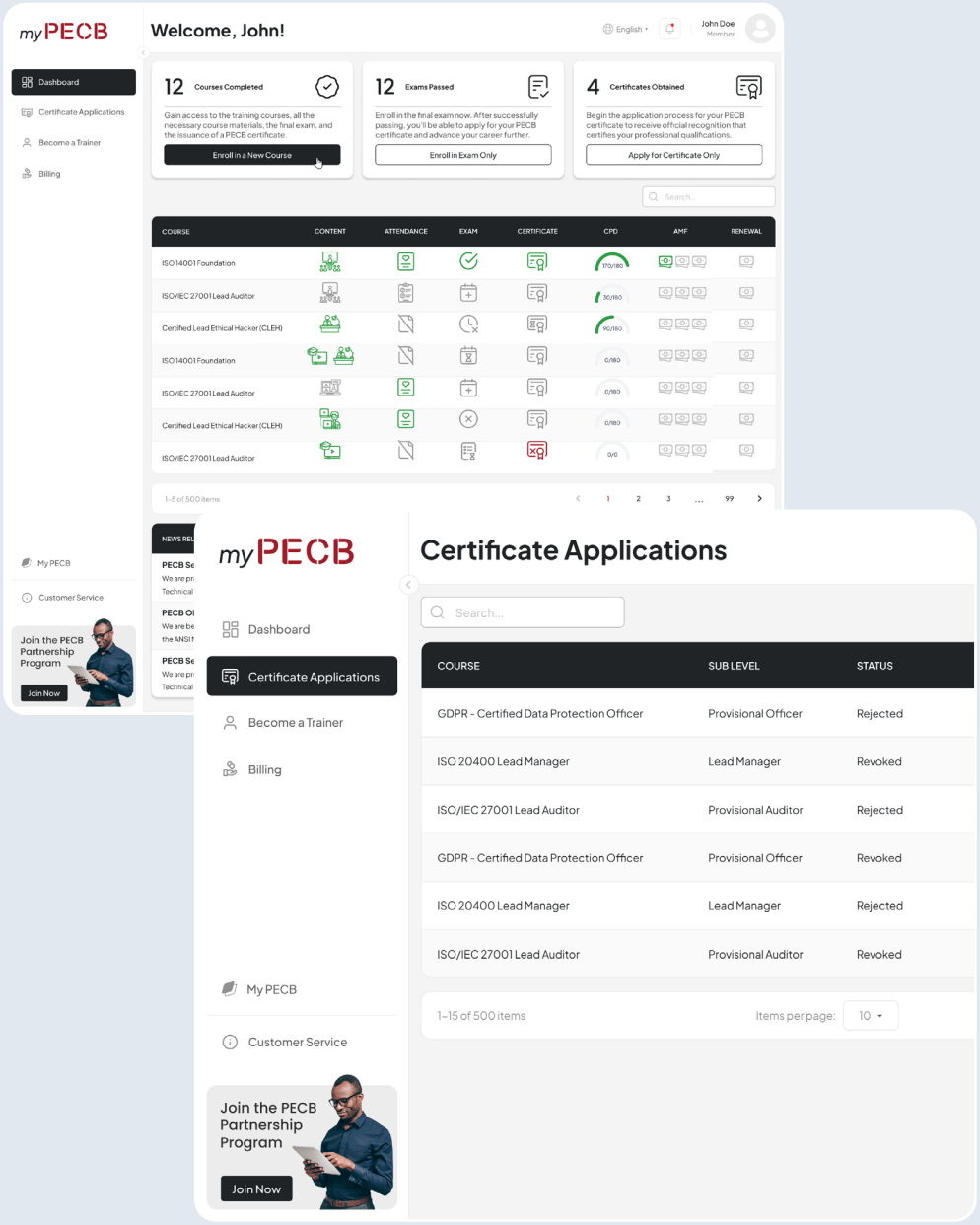
Dans son engagement envers l'innovation et l'excellence, PECB a lancé ***my*PECB**, une plateforme personnalisée et centralisée conçue pour améliorer l'expérience utilisateur et simplifier l'accès aux services de PECB.

Cette avancée offre un parcours numérique intuitif, efficace et engageant à notre communauté mondiale, garantissant que chaque interaction avec PECB soit simple, fluide et centrée sur l'utilisateur.

Présentation de myPECB – Votre hub numérique tout-en-un

- → Accéder à des **tableaux de bord personnalisés** adaptés à leur rôle spécifique
- → Gérer facilement **les dossiers de formation, les supports de cours, les certificats et les résultats d'examen**
- → Rester informé grâce à **des mises à jour en temps réel** sur la disponibilité des formations et les événements à venir

Accéder au myPECB



Un site Web repensé pour une expérience utilisateur moderne

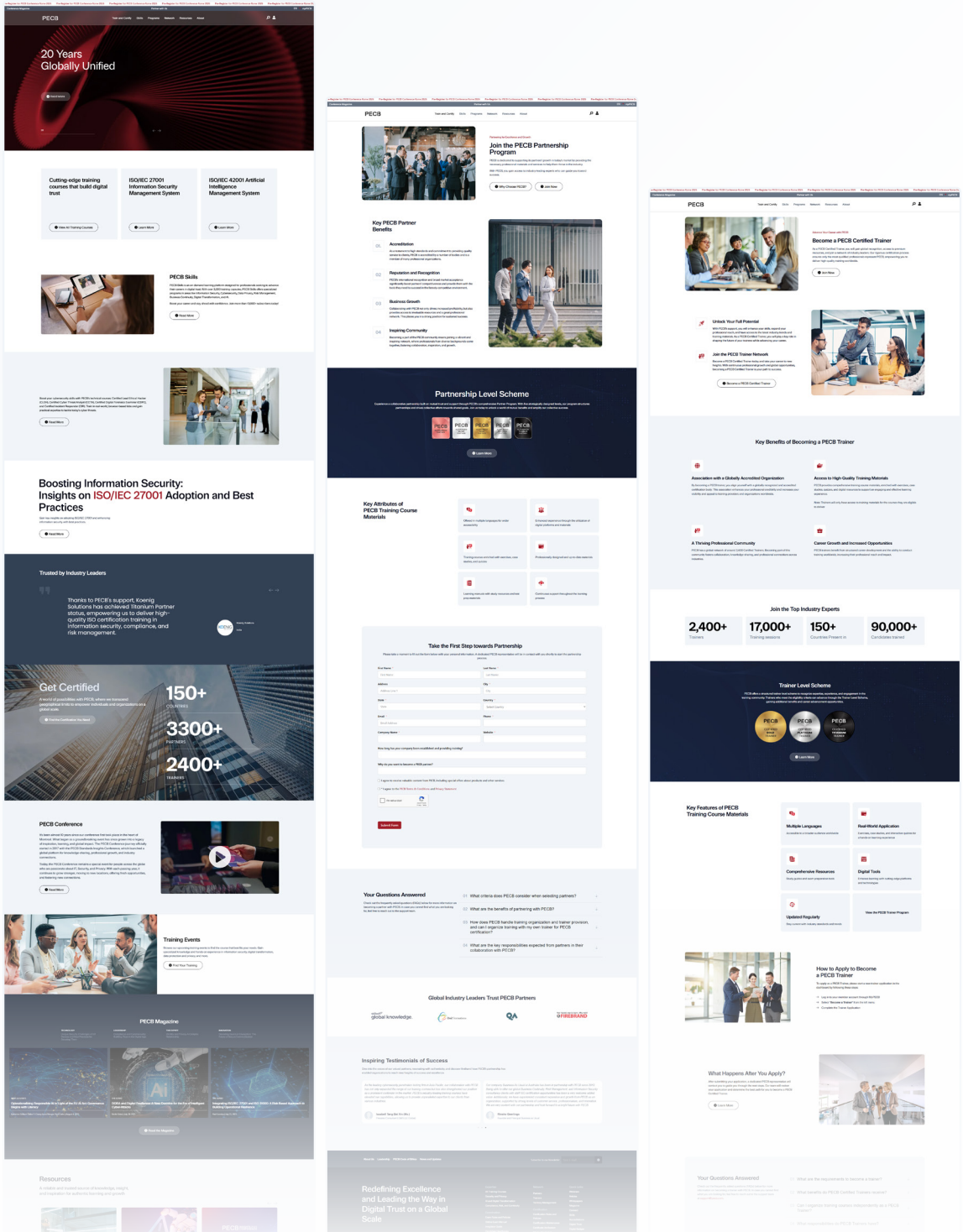
Complétant le lancement de *my*PECB notre site Web PECB a été entièrement repensé afin d'offrir une navigation plus rapide, plus claire et plus intuitive. La conception mise à jour garantit :

- → Navigation améliorée pour un accès rapide et facile aux informations
- → Structure optimisée et rapidité accrue pour une expérience sans interruption
- → Design modernisé reflétant notre vision tournée vers l'avenir

Un engagement envers l'innovation continue

Que ce soit pour gérer des certifications, s'inscrire à une formation ou découvrir davantage les services de PECB, le site Web repensé est conçu pour simplifier et améliorer l'expérience à chaque étape.

Découvrez le nouveau site Web



PECB Skills

Faire progresser les compétences en confiance numérique, une compétence à la fois.

PECB Skills est une plateforme dynamique de micro-apprentissage conçue pour les auditeurs, implementers et managers en sécurité de l'information, IA, protection de la vie privée et gouvernance des données qui ont besoin d'une formation rapide, pratique et fondée sur des normes.

Pourquoi choisir PECB Skills ?

Apprentissage dirigé par des experts :
Accédez à une bibliothèque complète de plus de 4 000 capsules vidéo interactives animées par des experts reconnus du secteur.

Thématiques complètes :
Explorez un large éventail de sujets, notamment la sécurité de l'information, le management des risques, le RGPD, l'IA, la cybersécurité, la conformité CMMC et bien plus encore.

Certification accréditée :
Obtenez des certificats dans le cadre de programmes de compétences sélectionnés accrédités par l'ANAB afin de mettre en valeur votre expertise.

Parcours structuré :
Suivez un parcours clair, des capsules aux modules et aux certificats de compétence.

Expérience interactive :
Participez à des leçons dynamiques, des quiz et des activités pratiques.

Crédits FPC :
Maîtrisez des compétences essentielles dans un programme de 4 heures et obtenez 4 crédits FPC.

Apprentissage flexible :
Conçu pour les professionnels du secteur, les dirigeants, les formateurs et les équipes.

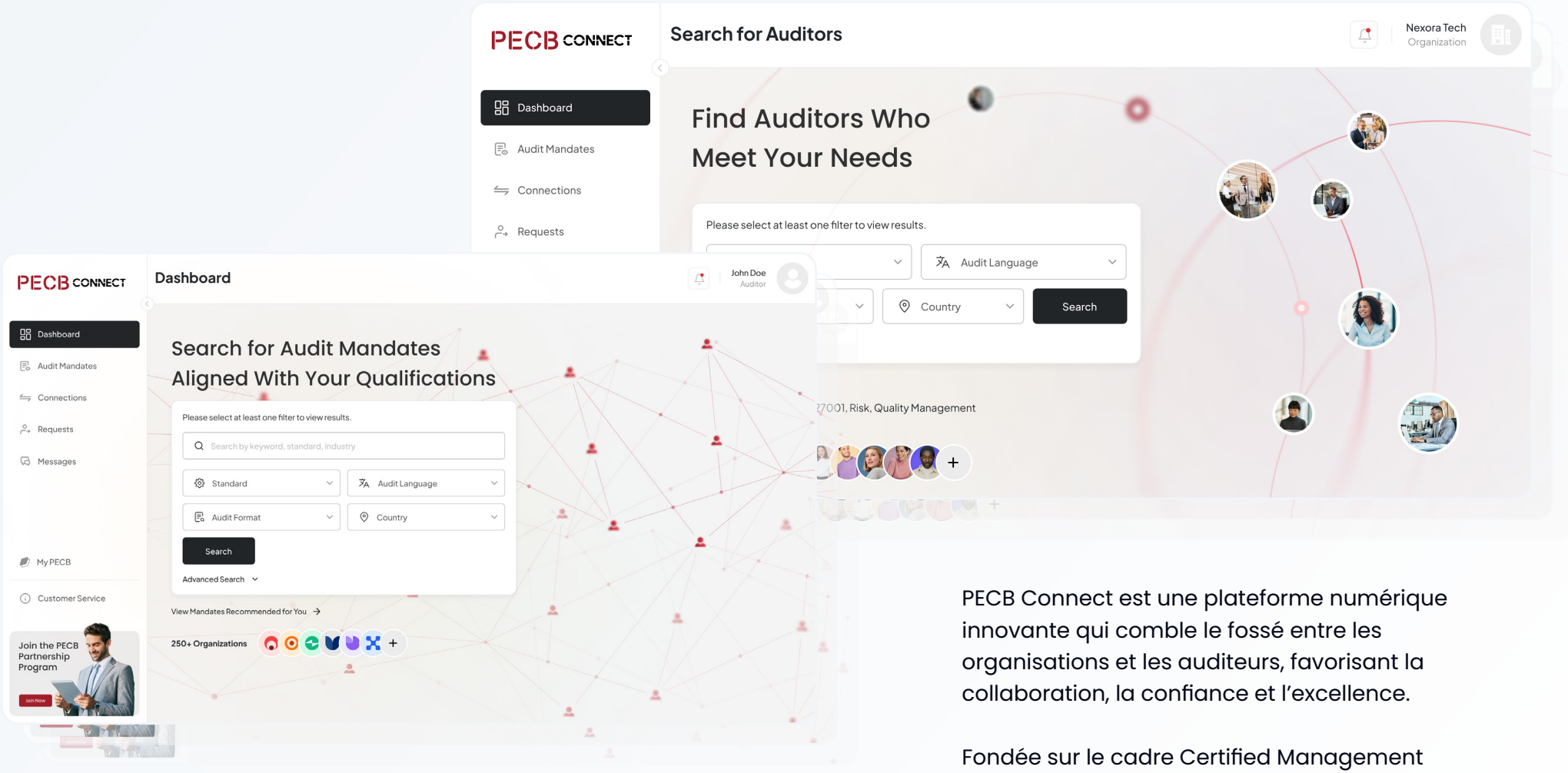
Suivi des progrès :
Suivez votre parcours d'apprentissage grâce à des analyses intuitives.

PECB Skills combine un contenu de pointe avec une plateforme conviviale afin d'offrir une expérience d'apprentissage fluide.
Que vous souhaitiez faire progresser votre carrière, obtenir des certifications, acquérir des crédits FPC ou approfondir votre expertise, PECB Skills est votre partenaire en développement professionnel.

Explorer maintenant

PECB Connect

Créer un pont entre les auditeurs et les organisations



PECB Connect est une plateforme numérique innovante qui comble le fossé entre les organisations et les auditeurs, favorisant la collaboration, la confiance et l'excellence.

Fondée sur le cadre Certified Management Systems Auditor (CMSA), PECB Connect offre un moyen transparent et efficace de se connecter, de collaborer et de réaliser des audits à l'échelle mondiale.

Pourquoi rejoindre PECB Connect ?

POUR LES ORGANISATIONS

Trouvez et contactez facilement des auditeurs qualifiés répondant aux besoins de votre organisation. Rejoignez PECB Connect pour simplifier la recherche de professionnels pour la certification, la conformité ou les audits internes.

Voici ce à quoi vous pouvez vous attendre :

- → Accès aux auditeurs : Entrez en contact avec des auditeurs formés, certifiés et évalués, garantissant le plus haut niveau de compétence et de professionnalisme.
- → Recherche simplifiée d'auditeurs : Utilisez des filtres avancés pour identifier des auditeurs selon les normes, l'expérience, la région ou le secteur, garantissant une adéquation parfaite pour chaque mandat d'audit.
- → Soutien à l'accréditation et à la conformité : PECB Connect aide les organisations dans le processus d'accréditation en facilitant l'accès à la documentation des auditeurs à des fins de conformité.
- → Cela simplifie la gestion des dossiers et facilite les rapports réglementaires.
- → Plateforme centralisée : Gérez toutes les relations avec les auditeurs, les communications et les mandats d'audit en un seul endroit. Trouvez facilement des auditeurs pertinents et qualifiés pour chaque mandat.

Pour rejoindre en tant qu'organisation, cliquez ici.

POUR LES AUDITEURS

PECB Connect est une plateforme conçue pour aider les auditeurs à entrer en contact avec des organisations ayant besoin de services d'audit.

Que vous soyez un auditeur expérimenté ou que vous débutiez votre carrière, cette plateforme vous donne accès à des projets d'audit disponibles et à des organisations recherchant des professionnels pour réaliser des audits.

Voici comment vous en bénéficiez :

- → Visibilité accrue : Les auditeurs bénéficient d'une exposition à un réseau élargi d'organisations recherchant des services d'audit.
- → Accès à un réseau mondial : PECB Connect met en relation les auditeurs avec des organisations du monde entier, leur permettant d'élargir leur portée et de collaborer à l'échelle internationale.
- → Opportunités ciblées : Les auditeurs reçoivent des opportunités adaptées à leur expertise, leur localisation, leur langue et d'autres critères, facilitant la recherche de mandats d'audit pertinents.
- → Processus simplifié de mise en relation : Le système structuré de la plateforme facilite la mise en relation des auditeurs avec des organisations recherchant une expertise spécifique, faisant gagner du temps aux deux parties.

PECB Connect offre aux organisations et aux auditeurs un environnement fiable, efficace et collaboratif afin de renforcer l'écosystème de certification et de promouvoir l'excellence professionnelle continue.

Pour rejoindre en tant qu'auditeur, cliquez ici.

Examen et certification

L'examen constitue l'étape clé du parcours de certification PECB, et nos examens sont conçus pour évaluer votre esprit critique et vos compétences en résolution de problèmes.

Disponibles dans le monde entier par l'intermédiaire de partenaires et distributeurs reconnus, nous proposons deux formats pratiques pour répondre à vos besoins :

- En ligne
- En format papier

Les types d'examen PECB

a) Questions à choix multiples, à livre fermé, où les candidats ne sont pas autorisés à utiliser des documents de référence. En général, les examens Foundation et Transition font partie de ce type.

b) Examens de type dissertation, à livre ouvert, où les candidats sont autorisés à utiliser les documents de référence suivants :

- Une copie papier de la norme principale
- Supports de formation (imprimés)
- Notes personnelles prises pendant la formation
- Dictionnaire au format papier

c) Examen à choix multiple et à livre ouvert, où les candidats sont autorisés à utiliser les documents de référence suivants :

- Une copie papier de la norme principale
- Supports de formation (imprimés)
- Notes personnelles prises pendant la formation
- Dictionnaire au format papier

Les examens sont disponibles en ligne via l'application PECB Exams. L'utilisation d'appareils électroniques secondaires, tels que tablettes et téléphones, n'est pas autorisée pendant l'examen. La session d'examen est supervisée à distance par un surveillant PECB grâce à l'application PECB Exams à l'aide d'une caméra externe ou intégrée.

Remarque : *Les examens de type dissertation à livre ouvert sont progressivement supprimés au profit des examens à choix multiples à livre ouvert. Les examens à livre ouvert comportent des questions basées sur des scénarios évaluant la capacité des candidats à appliquer, analyser et évaluer efficacement les informations.*

Selon le type de schéma d'examen, la durée varie :

Examens Foundation	**1 heure**
Examens Manager	**2 heures**
Examens Lead	**3 heures**
Examens techniques en cybersécurité	**6 heures**

Remarque : Les examens en ligne et sur papier ont la même durée que celle indiquée ci-dessus.

Pour commencer le processus et participer à nos formations, vous pouvez :

- Trouver un prestataire de formation dans votre région en consultant notre liste de partenaires.
- Vous inscrire à une formation et à un examen PECB via notre calendrier des événements de formation.
- Consulter la liste des examens PECB.

IMPORTANT : *Lors de votre préparation à l'examen, veuillez vous référer uniquement à notre site Web officiel pour les manuels candidats et les informations relatives aux examens. Veuillez éviter d'utiliser des sites non officiels de partage de sujets d'examen ou toute source tierce non autorisée. L'utilisation de tels supports peut entraîner de graves conséquences, notamment la non-validation de l'examen ou la révocation des certifications.*

Règles et politiques de certification PECB

Chaque certification PECB comporte un ensemble d'exigences.

Les candidats doivent compléter le formulaire de demande de certification en ligne ainsi que tous les autres formulaires en ligne, y compris les coordonnées des références qui seront contactées afin de valider l'expérience professionnelle des candidats.

Pour plus d'informations, veuillez consulter les Règles et politiques de certification.

Politique de maintien de la certification PECB

Les certifications PECB sont valables trois ans.

Pour maintenir une certification, les professionnels certifiés PECB doivent se conformer aux exigences suivantes :

- Soumettre des crédits de formation professionnelle continue (FPC)
- Payer les frais annuels de maintien (FAM)
- Adhérer au Code de déontologie de PECB

Pour renouveler une certification, les professionnels certifiés PECB devront démontrer qu'ils maintiennent leur certification en soumettant des unités FPC et en payant les FMA tout au long du cycle de certification de trois ans.

Une fois ces exigences satisfaites, votre certification sera renouvelée à la fin de la troisième année.

Remarque : *La certification CNIL a des exigences de renouvellement différentes. Les titres suivants ne nécessitent pas de maintien : Foundation, Provisional et Transition.*

Pour plus d'informations, veuillez consulter la politique de maintien des certifications.

Remise sur les FAM

Pour faciliter et simplifier le paiement des FAM, nous proposons les avantages suivants :

Remise de 10 % pour paiement anticipé

Vous pouvez choisir de payer trois années de FAM à l'avance et bénéficier d'une remise de 10 %. Ainsi, vous éviterez les paiements annuels pendant les trois prochaines années.

Plafond des FAM

Quel que soit le nombre de certifications détenues, vous ne serez tenu de payer des FMA que pour un maximum de **cinq certifications par an.**

eLearning

Une plateforme exclusive sur mesure adaptée à votre style d'apprentissage

La plateforme eLearning de PECB propose des formations en ligne personnalisées conçues pour s'adapter à différents styles d'apprentissage et modes de vie. Cette méthode d'enseignement numérique améliore l'efficacité et la qualité de l'apprentissage, en répondant à diverses préférences. Elle donne accès à des supports de formation complets élaborés avec la contribution de professionnels et de formateurs expérimentés dans divers domaines.

Pourquoi choisir l'eLearning de PECB ?

Accès aux formations 24 h/24 et 7 j/7
Apprenez à votre rythme, à tout moment et en tout lieu — sans contrainte d'horaire, de déplacement ou d'engagement professionnel.

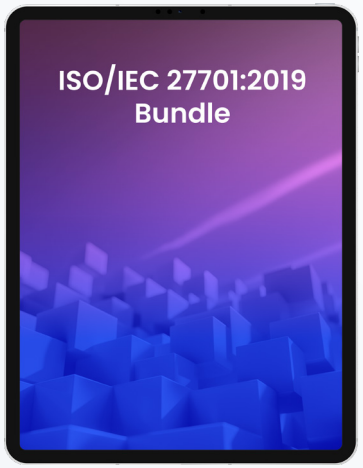
Contenu élaboré par des experts
Bénéficiez de supports développés par des professionnels disposant d'une expérience concrète dans leur domaine.

Leçons vidéo concises de 20 minutes
Modules courts et ciblés conçus pour faciliter l'apprentissage et améliorer la rétention.

Accès illimité aux supports de formation
Accédez à des ressources d'apprentissage complètes, disponibles à tout moment pour référence ou révision.

Entièrement en ligne
Formez-vous, étudiez et passez même vos examens sans quitter le confort de votre domicile.

PECB Store



ISO/IEC 27701:2019
Pack

Le pack ISO/IEC 27701 comprend une boîte à outils, la norme et une formation introductive proposée par PECB.

Acheter maintenant **$665**

ISO/IEC 27001:2022
Norme

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences.

Acheter maintenant **$143**

Découvrez ce que contient PECB Skills

Explorez et achetez des ressources de haute qualité, des boîtes à outils et eBooks à des milliers de normes ISO et IEC, afin de soutenir votre formation et votre développement professionnel.

*Accédez instantanément à tout, directement depuis votre tableau de bord my*PECB.

- → Un identifiant
- → Un hub central
- → Un parcours fluide

*my*PECB

PECB GDPR Implementation Toolkit

Cette boîte à outils propose des stratégies efficaces pour attribuer des rôles et répondre efficacement aux exigences en matière de protection des données.

Acheter maintenant **$495**

+1-844-426-7322 support@pecb.com www.pecb.com