Chartered Managers
EXPERTS ASSOCIES

PECB BEYOND RECOGNITION

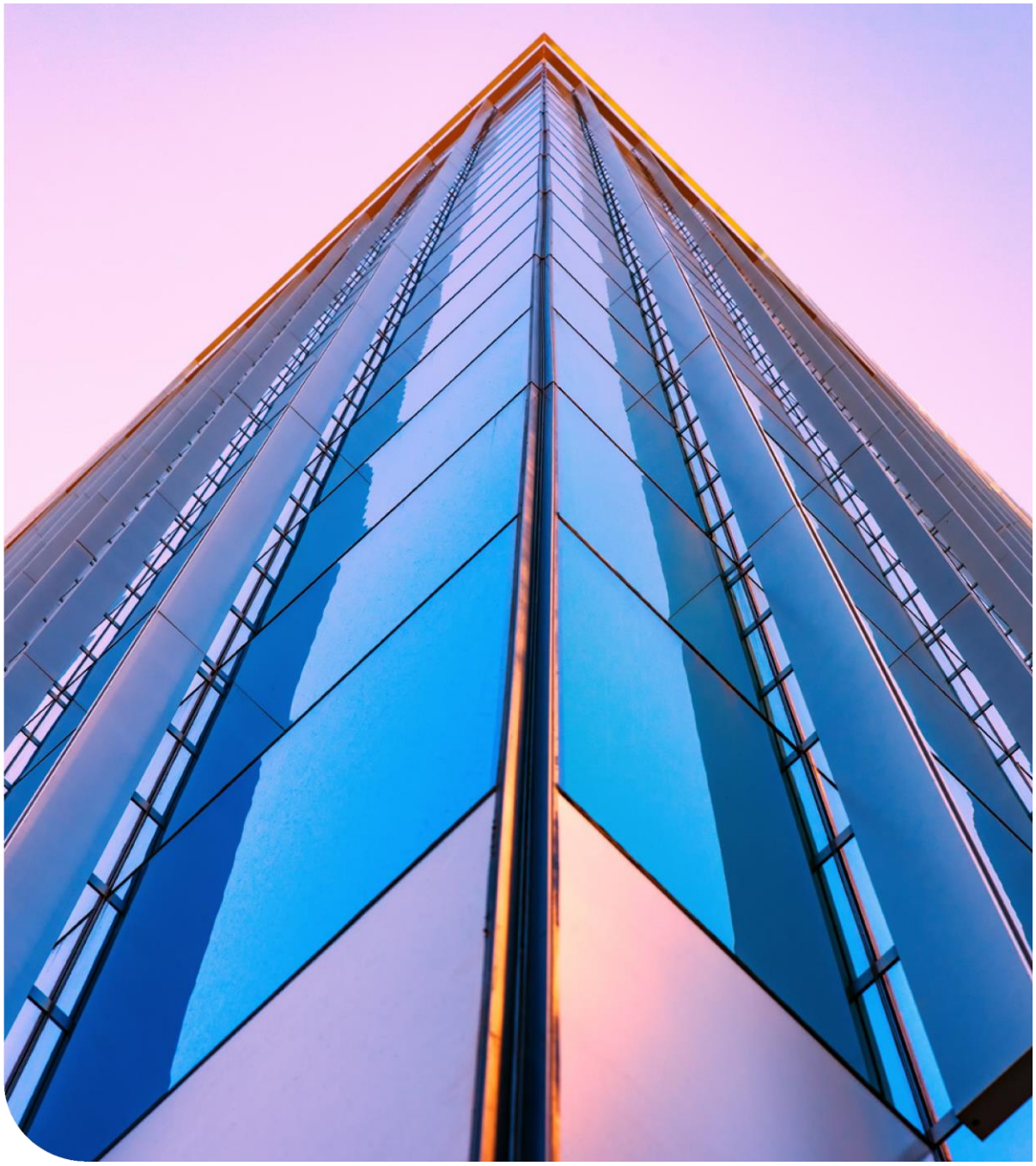
Guide des **Formations et Certifications Officielles Accréditées par PECB**

Faites progresser votre carrière grâce aux Certifications PECB reconnues mondialement dans les domaines des Systèmes de Management ISO, de la Cybersécurité, de la Gouvernance de l'IA, du RGPD, du Risque et de la Conformité.

Tout ce que vous devez savoir au sujet des Formations et Certifications PECB délivrées par *Chartered Managers*

Donner aux professionnels les moyens de réussir est au cœur de la mission de PECB, reflétant notre engagement envers l'excellence dans tout ce que nous entreprenons. Grâce à des services innovants et à une veille constante des évolutions du secteur, nous fournissons à nos clients les outils nécessaires pour dépasser leurs objectifs professionnels. Convaincus du pouvoir transformateur de l'apprentissage continu, notre engagement en faveur de la qualité, de la pertinence et de l'application pratique garantit que chaque service que nous offrons se traduit par un succès concret sur le terrain.

ERIC LACHAPELLE
Chairman at PECB



Chez PECB, nous croyons profondément au pouvoir transformateur du savoir et à la philosophie de l'amélioration continue. Nous encourageons et cultivons activement une culture d'exploration et d'apprentissage, en proposant un large éventail d'opportunités de développement personnel et professionnel.

Notre mission fondamentale est de doter les individus de compétences solides et d'une expertise de pointe afin de leur permettre d'exceller dans un environnement mondial en constante évolution.

Rejoignez-nous dans ce parcours — un parcours de croissance continue et de transformation. Chaque interaction avec PECB va bien au-delà d'une simple expérience d'apprentissage ; elle constitue une étape déterminante vers la réalisation de vos ambitions..

FATON ALIU
President, PECB

Bienvenue aux Programmes de Formation et Certifications PECB par CHARTERED MANAGERS !

Table des matières

Accréditation

L’accréditation est une **validation formelle par une autorité indépendante** qui certifie qu’un organisme est compétente, fiable, et respecte des exigences reconnues et normes spécifiques pour exercer une activité donnée (souvent internationales).

Elle permet de :

- Garantir la **qualité et la crédibilité** des services
- Rassurer les clients, partenaires ou autorités
- Assurer le respect de **normes internationales** (ISO, etc.)
- Donner une **valeur officielle** aux certifications ou formations délivrées

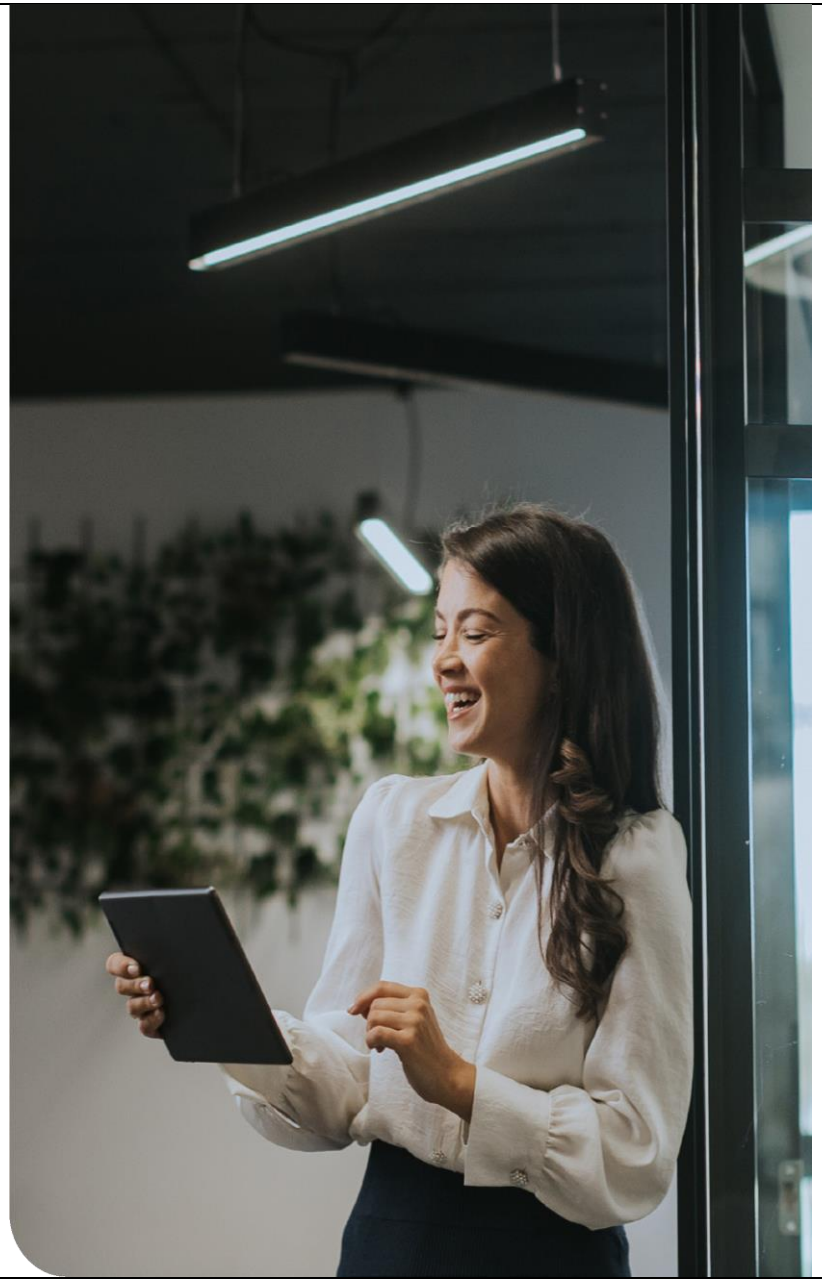
Certification

Procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus ou un service est conforme aux exigences spécifiées dans un référentiel

Différence importante

Accréditation → concerne les organismes (ex : organismes de certification, cabinets, centres de formation)

Certification → concerne les produits, services ou personnes



A propos de nous

PECB (Professional Evaluation and Certification Board) est un organisme de certification de personnes, de systèmes de management et de produits sur un large éventail de normes internationales. En tant que fournisseur mondial de formations, d'examens et de certifications, nous permettons aux professionnels de développer et de démontrer leurs compétences en matière de sécurité numérique et d'autres domaines d'expertise en proposant des programmes de certification de classe mondiale qui adhèrent à des normes internationalement reconnues.

La valeur des certifications PECB est reconnue à travers diverses accréditations et affiliations : https://pecb.com/fr/about/accreditations-and-affiliations

Depuis **2016**, **CHARTERED MANAGERS** est devenu partenaire **PECB** pour le **Moyen-Orient et l'Afrique**. Nous avons étendu nos activités à **l'Europe et à l'Amérique du Nord en 2021,** puis à la région **Asie-Pacifique en 2022**, et enfin à **l'Amérique latine (LATAM)** en 2024.

Cette expansion repose sur notre confiance dans l'expertise de PECB pour offrir des formations certifiantes de haute qualité dans des domaines essentiels tels que la sécurité de l'information, la continuité d'activité, la gouvernance, la gestion des risques, la conformité, la protection des données, la transformation digitale et l'intelligence artificielle. En tant que Partenaire PECB, nous sommes habilités à offrir les formations de certification PECB à l'échelle mondiale.

Ces formations ISO sont dispensées par de formateurs experts qui sont certifiés dans les normes qu'ils enseignent et ont travaillé dans le domaine. Ils partagent leurs idées, leur expérience et leurs connaissances sur la manière de mettre en œuvre ou d'auditer la norme ISO et encouragent toujours les participants à partager leurs points de vue et leurs idées

PRESENTATION DU CABINET

CHARTERED MANAGERS est un Cabinet international de Conseil, d'Audit, de Formation, composé d'un noyau d'experts pluridisciplinaires, qui ont décidé de mettre la somme de leurs savoir-faire, expériences, et expertises au service des entreprises, administrations, ONG et organisations internationales.

Grace à une approche intégrée et orientée résultats, le Cabinet propose des solutions pratiques, performantes et conformes aux standards internationaux, répondant aux exigences de gouvernance, d'efficacité et de performance durable afin d'accompagner les entreprises et les administrations publiques dans toutes les étapes de leur développement : de la stratégie à la mise en œuvre opérationnelle, en passant par le renforcement des capacités et la digitalisation des processus,

Fort de cette expertise éprouvée et de son dynamisme, **CHARTERED MANAGERS** s'est imposé au fil des années comme un **partenaire stratégique incontournable** pour l'**optimisation des ressources** et la **performance organisationnelle** des entreprises, administrations publiques, ONG, institutions internationales.

UNE EXPERTISE INTEGREE AUTOUR DE CINQ POLES MAJEURS :

1/ AUDIT - CONSEIL STRATEGIQUE ET OPERATIONNEL :
Accompagnement des organisations dans l'élaboration et la mise en œuvre de stratégies de croissance, de performance et d'optimisation des processus.

2/ INGENIERIE DE FORMATION :
Un **catalogue riche et varié** couvrant **tous les domaines fonctionnels de l'entreprise** *(Achats /Logistique, Ressources Humaines, Management et Leadership, Marketing, Comptabilité, Gestion et Finance, Droit, fiscalité, Informatique, QHSE, Gestion de Production, Gestion de Projets, Gouvernance-Risques-Conformité, IT, Cybersécurité, Digital & IA, etc.).* Nos programmes couvrent également les **spécificités métiers** : banques et assurances, ONG et projets de développement, secteur public, BTP, immobilier, grande distribution, activités portuaires et maritimes.

3/CERTIFICATIONS INTERNATIONALES :
Chartered Managers propose en partenariat avec plusieurs organismes de certification **près de 150 formations certifiantes** permettant d'obtenir des **titres et certifications reconnus mondialement,** gages d'expertise technique et de crédibilité professionnelle : **Management & Gouvernance :** PMP®, PMD Pro, PRINCE2™, AgilePM®, Lean Six Sigma (Yellow/Green/Black Belt), COBIT® 2019, ITIL®, CISA®, CISSP - **Technologies & Réseaux :** CISCO (CCNA, CCNP, CCIE), Big Data, Cloud, Sécurité Informatique, DevOps - **Normes & Qualité :** ISO 9001, ISO 14001, ISO 45001, ISO 22000, ISO 28000, ISO 27001, ISO 42001, ISO 37000, ISO 17025, ISO 37301, etc.). Ces certifications, obtenues grâce à nos partenariats avec des organismes de référence, renforcent la **valeur des profils formés** et leur **employabilité sur le marché international** .

4/ APPUI AUX PROJETS DE DEVELOPPEMENT:
Assistance technique auprès des acteurs du secteur public, privé et humanitaire, notamment dans la conception, la gestion et l'évaluation de projets et programmes.

5/ INNOVATION ET DIGITALISATION :
Intégration des outils numériques modernes (marketing digital, communication digitale, gestion des données & Intelligence Artificielle) afin d'accompagner les organisations dans leur transition digitale.

NOTRE FORCE REPOSE SUR :

✅ **Une équipe pluridisciplinaire et multiculturelle de 160 EXPERTS ET DE FORMATEURS CERTIFIES**, présents en Afrique, en Europe, et en Amérique du Nord, disponibles. Ils allient expérience métier et expérience en consulting, en audit, et en formation.
✅ **Des solutions** adaptées aux réalités des entreprises africaines et aux standards internationaux
✅ **Une vision** internationale soutenue par des partenariats et collaborations internationales
✅ **Un engagement** ferme pour l'innovation, la qualité et l'excellence opérationnelle.

NOS HUBS DE FORMATION

Douala (Cameroun) • **Montréal** (Canada) • **Paris** (France) • **Abidjan** (Côte d'Ivoire) •**Dubaï** (UAE) • **Dakar** (Sénégal) • **Casablanca** (Maroc) • **Kinshasa** (Congo)) • **Cotonou** (Bénin) - **Intervention dans vos locaux partout en Afrique**.

Accréditations et affiliations de PECB

En témoignage des normes élevées et de l'engagement à fournir un service de qualité aux clients, PECB est accrédités par un certain nombre d'organismes et membres de nombreuses organisations professionnelles énumérées ci-dessous :

- **Accrédité par l'IAS en tant qu'Organisme de certification de personnes :**PECB est un organisme de certification de personnes accrédité par le International Accreditation Service (IAS) selon la norme ISO/IEC 17024 − Exigences générales pour les organismes procédant à la certification des personnes.

- **Accrédité par UKAS comme organisme de certification de personnes :** PECB est accrédité par l'United Kingdom Accreditation Service (UKAS) selon la norme ISO/IEC 17024 — Évaluation de la conformité — Exigences générales pour les organismes de certification procédant à la certification de personnes.

- **Accréditation par le Comité Français d'Accréditation (COFRAC) :** PECB est accrédité par le Comité Français d'Accréditation (COFRAC) selon la norme ISO/IEC 17024 – Évaluation de la conformité – Exigences générales pour les organismes de certification de personnes.

- **Accrédité par l'ANAB en tant que fournisseur de certificats :** PECB est accrédité par l'ANSI National Accreditation Board (ANAB) conformément à la norme ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

- **Membre associé de la Independent Association of Accredited Registrars (IAAR) :** PECB est un membre associé de l'Independent Association of Accredited Registrars (IAAR).

- **Membre signataire de l'association International Personnel Certification (IPC) :** PECB est membre à part entière de l'association International Personnel Certification (IPC) et membre signataire de l'IPC MLA.

- **Accrédité et membre du Club EBIOS :** PECB est membre du Club EBIOS et le premier organisme de certification accrédité par celui-ci.

- **Approuvé Approved Publishing Partner (APP) par l'organisme d'accréditation CMMC :** PECB est agréé en tant que Approved Publishing Partner (APP) par le Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) pour la norme de certification Cybersecurity Maturity Model Certification (CMMC).

- **Distributeur autorisé du Standards Council of Canada - Conseil canadien des normes (SCC) :** PECB est un distributeur du Conseil canadien des normes autorisé à commercialiser et à vendre les normes ISO et IEC par le biais de sa boutique en ligne.

- **Accrédité par et membre du CPD Certification Service ;** PECB est membre du CPD Certification Service. De plus, le CPD Certification Service a certifié le contenu de 10 formations PECB comme étant conforme aux principes de formation professionnelle continue.

- **Membre du CLUSIF :** PECB devient membre du CLUSIF (Club de la Sécurité de l'Information Français).

- **PECB est agréé par la CNIL pour offrir la certification de DPO :** PECB est agréé par la Commission Nationale de l'Informatique et des Libertés (CNIL), pour proposer des services de certification des compétences et des connaissances des délégués à la protection des données (DPO) sur la base du schéma de la CNIL, conformément aux délibérations de la CNIL n° 2018-317 et n° 2018-318 du 20 septembre 2018

Nos valeurs

Toujours Disponibles, Et A L'écoute	Accompagnement Complet	Engagement De Résultat
C'est par des relations professionnelles basées sur l'écoute, la transparence et la réactivité que notre collaboration est dynamique et efficace. Le tout, dans la bonne humeur !	Parce que chaque client est unique, l'ensemble de nos accompagnements sont sur-mesure. - Un seul consultant Expert est dédié à votre projet de certification. - Lors de l'audit à blanc, nous proposons de faire intervenir un autre consultant auditeur de notre cabinet, sur la norme concernée, pour une vision externe et mise en situation réelle de votre audit final de certification.	C'est par nos acquis, notre exigence de qualité et notre engagement contractuel de résultat que nous conservons la confiance de nos clients. - Nous disposons également d'un fort taux de recommandations et de réengagement (suivi ou externalisation de la prestation de la fonction de Responsable QHSE

Ce que nous faisons

Formations	Conseil & Accompagnement	Audit
Nous proposons des formations certifications aux professionnels conformément aux normes internationales . Nous sommes le cabinet partenaire privilégié de PECB, un fournisseur mondial de services de certification professionnelle.	Nos consultants certifiés aideront votre organisation à établir, mettre en œuvre, gérer et améliorer vos systèmes de management Nous vous proposons des solutions complètes ou des services ad-hoc selon le contexte et les besoins de votre organisation.	Nos auditeurs vous guideront tout au long du cycle d'audit. Ils vérifieront le niveau de conformité aux exigences des normes et procédures internes, aux lois, règlements, obligations contractuelles ainsi que l'efficacité des contrôles en place. Vous recevrez des recommandations pour le traitement des non-conformités et l'amélioration de l'efficacité des systèmes de management et des mesures associées.

Pourquoi Choisir PECB ?

Fournisseur des services de formation, d'examen et de certification

La firme Canadienne PECB (Professional Evaluation And Certification Board) est un organisme de certification procédant à la certification des personnes, des systèmes de management, et des produits pour un large éventail de normes internationales. En qualité de prestataire mondial de formations, d'examens, d'audits, et de services de certification, PECB offre son expertise dans de multiples domaines.

Par sa présence mondiale, PECB offre des services de certification aux meilleurs des professionnels à travers le monde en proposant d'excellents programmes avec des méthodologies éprouvées et des normes internationalement reconnues, lesquelles sont réputées comme un moyen de promouvoir les compétences professionnelles dans un cadre exhaustif de bonnes pratiques.

Les formations agréées PECB vous permettront d'acquérir les meilleures pratiques de l'industrie et de comprendre comment les changements peuvent affecter le système de management de votre organisation

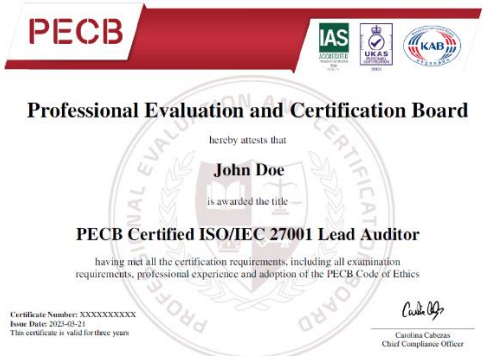
La réponse en 6 points :

1. **PECB est accrédité :** L'accréditation est indispensable pour la reconnaissance internationale de votre certification. C'est pourquoi le choix du bon organisme de certification est crucial pour votre réussite à court et à long terme, l'avenir de votre profession et les nombreuses opportunités qui vous attendent à l'échelle mondiale
2. **Reconnaissance mondiale :** Les certifications PECB sont très recherchées et directement applicables en milieu professionnel. PECB est présente dans plus de 150 pays dans le monde, à travers son réseau de revendeurs, de formateurs et de professionnels. Son accréditation, son large éventail de services couvrant de multiples domaines, ainsi que le succès des professionnels certifiés PECB sont la preuve de votre itinéraire vers la reconnaissance internationale.
3. **Les certifications de PECB sont acceptées partout :** Une certification PECB fournira l'opportunité aux professionnels de démontrer conformité, dévouement pour l'excellence et compétence dans l'amélioration des opérations des organismes dans le monde entier.
4. **Frais raisonnables :** . Les tarifs des formations PECB sont particulièrement compétitifs par rapport à de nombreuses autres certifications et incluent les frais d'examen. Avec PECB, il n'y a pas de coûts cachés.
5. **Meilleurs supports de formation de l'industrie :** Nos formations sont au cœur de l'innovation. Elles présentent les dernières normes ISO, les technologies les plus innovantes, les approches, les méthodes et les exemples pratiques les plus récents tout en étant précises, crédibles et utiles. Quel que soit votre domaine d'expertise, nous avons la formation qui vous convient, de la sécurité de l'information et de la continuité d'activité à la santé, la sécurité, la durabilité et bien plus encore. Étant à l'avant-garde du marché du point de vue du contenu, de la conception et de l'approche pédagogique, nos formations vous aident à améliorer vos compétences et vos connaissances et à développer la compétence nécessaire pour faire la différence dans votre industrie
6. **Réputation :** Les organismes sont jugés par de différentes façons : par ce qu'ils font, ce qu'ils disent faire, ou ce que les autres disent qu'ils font. En ce qui concerne la perception de la valeur, la bonne réputation des certifications PECB nous a aidés à acquérir un avantage concurrentiel. Nous en voulons pour preuve les professionnels certifiés PECB qui font partie des marchés les plus prospères du monde entier en adoptant une culture en constante amélioration

Quelle est la valeur de la certification PECB ?

La valeur et la reconnaissance de la certification professionnelle ne cessent de gagner en importance dans un monde en constante évolution. Cela étant, le choix d'opter pour une certification de ses compétences pour une norme particulière est également simplifié.

Un nombre croissant de professionnels ont compris et apprécié aujourd'hui à sa juste valeur le fait que les bonnes pratiques et les méthodes pour un domaine donné existent. Cette prise de conscience est intervenue par l'application des savoirs et des compétences acquis en formation au service des objectifs de leur entreprise, devenant ainsi le facteur clé de la réussite de leur organisation.


PECB

Professional Evaluation and Certification Board

hereby attests that

John Doe

is awarded the title

PECB Certified ISO/IEC 27001 Lead Auditor

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: XXXXXXXXX
Issue Date: 2022-05-21
This certificate is valid for three years

Carolina Cabezas
Chief Compliance Officer

Lorsqu'une organisation recrute un expert en sécurité de l'information, un gestionnaire de risque, un gestionnaire de projet, un manager qualité, sécurité, environnement..., **votre qualification et votre expérience dans ce domaine est une composante importante de votre valeur ajoutée à votre employeur mais elle n'est pas suffisante.**

En effet, les entreprises ont besoin de quelque chose de quantifiable et de vérifiable pour leur montrer que vous avez l'expertise qu'ils recherchent. **Par conséquent, la préférence va au candidat qui est titulaire de la certification professionnelle adéquate, qu'il s'agisse d'une certification ISO/IEC 27001 Sécurité de l'information, d'une certification ISO 31000 Manager de risque, d'une certification ISO 21500-management des projets, ou d'une certification de management de la qualité ISO 9001.**

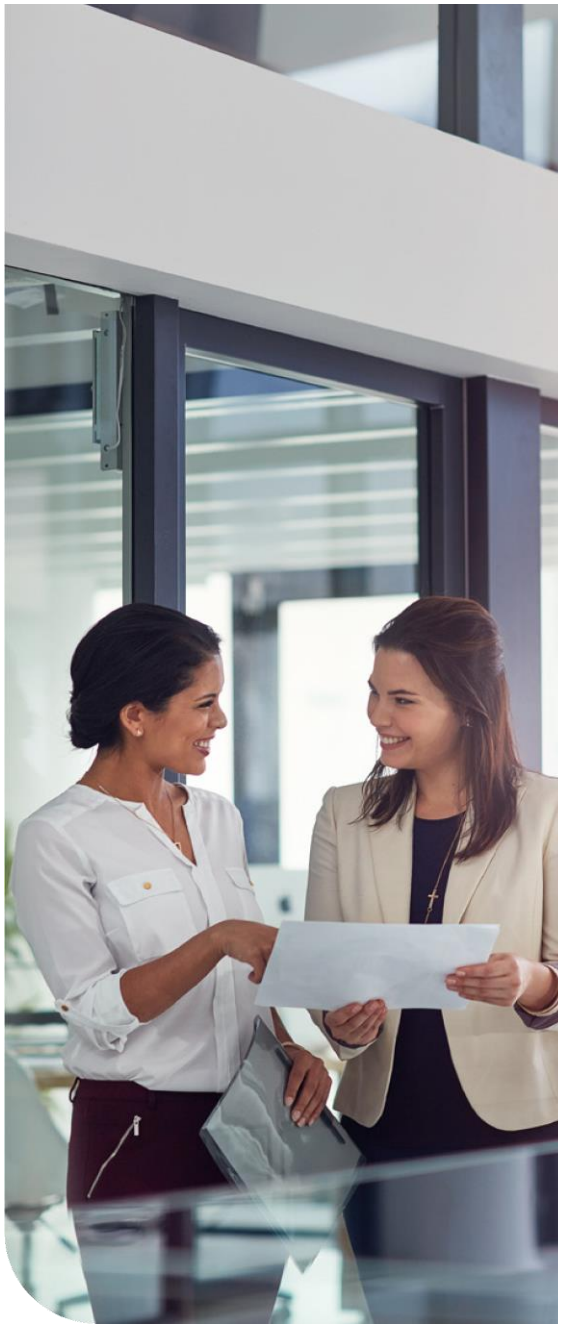
Toutefois, la certification professionnelle ne se limite pas à l'obtention d'un certificat qui confirme la réussite d'une formation ; mais doit être interprétée comme l'attestation et la reconnaissance des compétences pratiques et du développement professionnel tout au long de l'expérience d'un professionnel. De la formation intégrale aux procédures d'examen rigoureuses, le candidat voit ainsi ses connaissances pratiques attestées et est reconnu comme un professionnel certifié.

Actuellement les postes dans beaucoup d'organismes privés ou publics requièrent une certification et les **praticiens certifiés ISO** disposent **des opportunités de carrière plus importantes**, et des revenus plus élevés. De plus, vous serez reconnus au niveau mondial comme appartenant à la communauté des experts de votre domaine, ce qui vous créditera d'une confiance nouvelle en vos capacités à réussir face aux situations difficiles rencontrées dans le monde du travail.

Au cœur de la mission de PECB se trouve l'engagement de transformer les individus en experts, tout en cultivant une culture de croissance continue. Notre vision va bien au-delà de la simple certification des compétences : nous aspirons à autonomiser les personnes par le savoir.

Ensemble, nous construisons un avenir où l'expertise rime avec émancipation et opportunités. À travers l'éducation, notre mission centrale est de contribuer à la création d'un monde offrant des perspectives illimitées à nos clients.

TIM RAMA
Chief Executive Officer at PECB



Portefeuille Diversifié de Formations Certifiées PECB

CHARTERED MANAGERS propose en partenariat avec PECB une large gamme de formations certifiantes réparties par domaines de spécialisation.

Ces programmes sont conçus pour aider les professionnels à développer des compétences et des connaissances pointues dans des secteurs spécifiques, tout en leur offrant une compréhension approfondie des normes et cadres de référence applicables.

Chaque programme est conçu pour offrir :

- ✔ une expertise approfondie
- ✔ des compétences pratiques et directement applicables
- ✔ une forte valeur ajoutée professionnelle

Les approches pédagogiques de PECB permettent aux participants de maîtriser la mise en œuvre et la gestion efficaces de ces pratiques au sein de leurs organisations, renforçant ainsi leur expertise dans leurs domaines respectifs.

Découvrez dans les pages suivantes un aperçu des formations proposées dans chaque portefeuille :

Les domaines d'intervention

CHARTERED MANAGERS a des expériences et compétences confirmées dans les domaines suivants :

MANAGEMENT DE LA QUALITE ET DES SERVICES

→ ISO 9001, Système de management de la qualité
→ Six Sigma
→ ISO 13485, Management de la Qualité des dispositifs médicaux
→ ISO/IEC 17025, Management des laboratoires
→ ISO/IEC 20000, Management de l'information
→ ISO 21001, Management des organismes d'éducation
→ ISO 21502 Système de management des projets
→ ISO 55001 Système de management des actifs
→ ISO 28000 Management de la sûreté et de la chaîne d'approvisionnement
→ ISO/TS 29001, Management de la qualité pour l'industrie du pétrole de la pétrochimie et du gaz naturel

SANTE ET SECURITE ET DURABILITE

→ ISO 45001 Système de management de la santé et de la sécurité au travail
→ ISO 22000 Management de la sécurité des denrées alimentaires
→ ISO 18788 Système de management des opérations de sécurité privées
→ ISO 39001, Management de la Sécurité Routière

DURABILITE

→ ISO 50001 Système de management de l'énergie
→ ISO 14001 Système de management environne mental
→ ISO 26000 Responsabilité Sociétale
→ ISO 37101 Développement durable dans les collectivités
→ ISO 20400 Lignes directrices pour les achats responsables

GOUVERNANCE, RISQUE, CONFORMITE

→ ISO 31000, Système de management des risques
→ ISO 37000, Gouvernance d'entreprise
→ ISO 37001, Système de management anti-corruption
→ ISO 37301, Système de management de la conformité
→ ISO/IEC 38500, Gouvernance Informatique
→ CMSIA, Auditeur Interne des Systèmes de Management Certifié
→ ORM, Gestion des Risques Opérationnels dans les Institutions Financières

RESILIENCE, CONTINUITE ET REPRISE D'ACTIVITE

→ ISO 22301, Management de la continuité d'activité
→ Disaster Recovery, Reprise d'activité après sinistre
→ DORA, Digital Operational Resilience Act, Résilience opérationnelle numérique
→ Operational Resilience Management, Gestion de la résilience opérationnelle
→ Crisis Management, Gestion des crises

SECURITE DE L'INFORMATION

→ ISO/IEC 27001, Management de la sécurité de l'information
→ ISO/IEC 27002, Contrôles de sécurité de l'information
→ EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
→ ISO/IEC 27005, Gestions des risques liés à la sécurité de l'information
→ ISO/IEC 27034, Sécurité des Application
→ ISO/IEC 27035, gestion des incidents de sécurité de l'information
→ CISO/RSSI, Chief Information Security Officer ou Responsable de la sécurité du système d'information
→ ISO/IEC 27400, Sécurité et Confidentialité de l'Internet des Objets (IoT)

GESTION DE LA CYBERSECURITE

→ Cybersecurity Management
→ Cloud Security
→ Penetration Testing / Test d'Intrusion
→ SCADA, Supervisory Control and Data Acquisition (Système de contrôle et d'acquisition de données)
→ CMMC, Cybersecurity Maturity Model Certification
→ NIS 2 Directive, directive (UE) 2022/2555
→ ISO/IEC 27033 Network Security
→ SOC 2 - Systems and Organization Controls
→ NIST Cybersecurity
→ ISA/IEC 62443, Systèmes d'Automatisation et de Contrôle Industriels

CYBERSECURITE TECHNIQUE

→ Ethical Hacking
→ CCTA, Certified Cyber Threat Analyst
→ Incident Response

PROTECTION DES DONNEES ET DE LA VIE PRIVEE

→ISO/IEC 27701, système de management de protection de la vie privée
→ RGPD, Reglement Général sur la Protection des Donnée

INTELLIGENCE ARTIFICIELLE

→ ISO/IEC 42001, Système de management de l'intelligence artificielle
→ CAIP, Artificial Intelligence Professional
→ CAIM, Artificial Intelligence Manager
→ CAIA, Artificial Intelligence Auditor
→ AI Risk Management

TRANSFORMATION NUMERIQUE

→ CDTO, Responsable Certifié de la Transformation Digitale
→ Digitalisation, Conservation & Archivage des données Numériques

Parcours de développement de compétences:

Niveaux de Formations et Durées

FORMATIONS SUR LES SYSTEMES DE MANAGEMENT	PUBLIC CIBLE	DUREE
FOUNDATION	• Personnes souhaitant 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 place et de la gestion d'un système de management au sein de leur organisation	**5 JOURS**
LEAD AUDITOR	• Personnes chargées d'auditer et de surveiller les systèmes de management	**5 JOURS**
FORMATIONS MANAGÉRIALES ET OPERATIONELLES	**PUBLIC CIBLE**	**DUREE**
FOUNDATION	• Personnes souhaitant étudier les fondamentaux des processus et procédures liés au domaine ou à la norme concernée	**2 JOURS**
MANAGER / OFFICER	• Managers souhaitant développer leurs compétences pour mettre en œuvre des processus, approches, techniques, programmes, plans et stratégies	**3 JOURS**
LEAD MANAGER / OFFICER	• Managers souhaitant évaluer, gérer ou maintenir des plans, cadres, programmes, etc., et renforcer leur expertise managériale	**5 JOURS**
FORMATIONS SPÉCIALISÉES (NON-ISO)	**PUBLIC CIBLE**	**DUREE**
FOUNDATION	• Personnes souhaitant étudier les bases du domaine concerné et ses processus associés	**2 JOURS**
MANAGER / OFFICER	• Managers souhaitant acquérir des connaissances sur les principes et concepts fondamentaux d'un programme de management	**3 JOURS**
LEAD MANAGER / OFFICER	• Managers souhaitant développer leurs compétences et connaissances dans le domaine concerné et renforcer leur expertise	**5 JOURS**
FORMATIONS TECHNIQUES EN CYBERSÉCURITÉ	**PUBLIC CIBLE**	**DUREE**
OFFENSIVE CYBERSECURITY	• Professionnels souhaitant mieux comprendre les tactiques et techniques utilisées par les hackers malveillants afin d'améliorer la protection de leurs systèmes	
DEFENSIVE CYBERSECURITY	• Personnes souhaitant renforcer significativement leurs capacités défensives et apprendre les meilleures pratiques de sécurisation des systèmes	
DIGITAL FORENSICS	• Professionnels souhaitant acquérir un large éventail de compétences essentielles en investigation et analyse numérique	

Votre Certification PECB, c’est Votre Crédibilité !

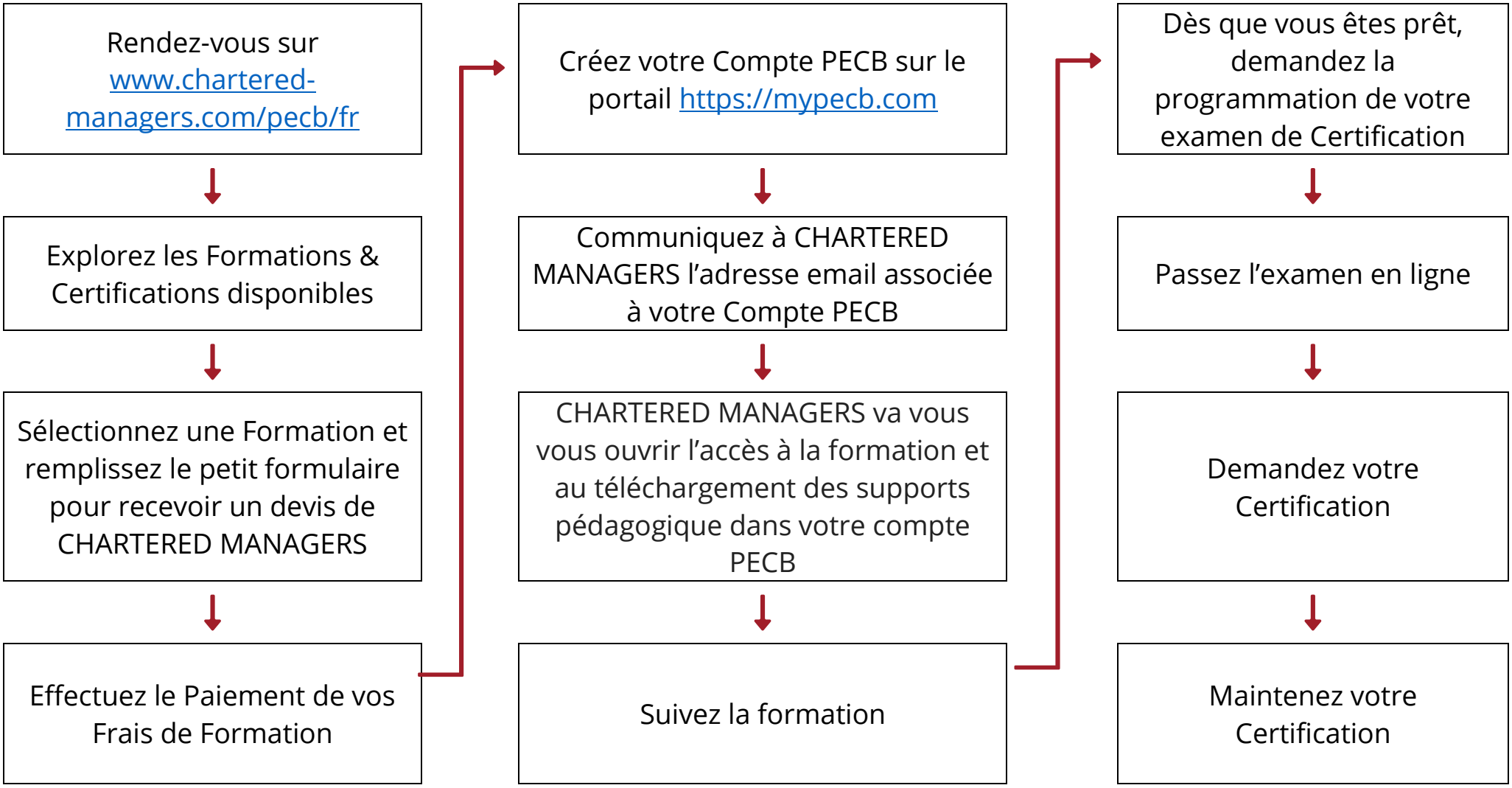
Une certification professionnelle est un gage de formation, de validation et de reconnaissance. Plus encore, les certifications délivrées par PECB démontrent que vous êtes un professionnel engagé dans votre développement et votre excellence. Elles attestent que vous avez acquis **des compétences et des connaissances reconnues et vérifiées.**

Que vous débutiez votre parcours ou que vous soyez déjà un expert confirmé dans le domaine des normes ISO et autres cadres réglementaires, une certification PECB renforce votre trajectoire professionnelle et maximise vos opportunités de réussite.

Nos certifications vous aident à mieux accomplir vos missions et constituent une preuve fiable que vous respectez les exigences minimales en matière de compétence professionnelle et d’éthique. Elles vous accompagnent également dans la maîtrise et la gestion efficace de l’ensemble de vos responsabilités.

Il s’agit d’un investissement précieux, à la hauteur de votre temps et de vos ressources — car la quête continue de connaissances est le moteur d’une carrière florissante et d’un développement professionnel durable.

Parcours du processus d'inscription à la certification



Commencez Maintenant :

https://www.chartered-managers.com/pecb/fr

Critères de Certification :

Désignation, Expérience et Exigences liées aux Projets

EXAMEN	CERTIFICATION	EXPERIENCE PROFESSIONNELLE	ACTIVITES D'AUDIT	EXPERIENCE EN PROJET
FOUNDATION	Foundation	Aucune	–	–
LEAD MANAGER	Provisional Manager	Aucune	–	–
	Manager	2 ans (1 dans le domaine de spécialisation)	–	200 heures
	Lead Manager	5 ans (2 dans le domaine de spécialisation)	–	300 heures
	Senior Lead Manager	10 ans (7 dans le domaine de spécialisation)	–	1,000 heures
LEAD AUDITOR	Provisional Auditor	Aucune	Aucune	–
	Auditor	2 ans (1 dans le domaine de spécialisation)	200 heures	–
	Lead Auditor	5 ans (2 dans le domaine de spécialisation)	300 heures	–
	Senior Lead Auditor	10 ans (7 dans le domaine de spécialisation)	1,000 heures	–
LEAD IMPLEMENTER	Provisional Implementer	Aucune	–	–
	Implementer	2 ans (1 dans le domaine de spécialisation)	–	200 heures
	Lead Implementer	5 ans (2 dans le domaine de spécialisation)	–	300 heures
LEAD AUDITOR & LEAD IMPLEMENTER	Senior Lead Implementer	10 ans (7 dans le domaine de spécialisation)	–	1,000 heures
	Master	20 ans d'expérience (dont 10 ans à un poste de leadership dans le domaine de spécialisation	10 000 heures cumulées d'activités d'audit et de gestion de projets	

Formats de Dispensation des Formations

Les différents modes de formation PECB dispensées par CHARTERED MANAGERS s'adaptent à une grande diversité de profils d'apprenants, garantissant accessibilité, flexibilité et qualité tout au long du processus de formation et de certification.

Présentiel

Participez à des sessions de formation interactives animées par des formateurs certifiés PECB, dans un environnement structuré en face à face, idéal pour l'application pratique des connaissances.

Classe Virtuelle

Bénéficiez de formations dynamiques et interactives, animées par des formateurs certifiés PECB, via Zoom accessible à tous, y compris aux professionnels disposant de contraintes de temps ou de déplacement.

eLearning

Formations flexibles et indépendantes du lieu, basées sur des vidéos préenregistrées. Elles incluent des quiz, des ressources complémentaires et des sessions de questions-réponses en direct (optionnelles).

Autoformation

Apprentissage à votre rythme, avec accès aux supports de cours. Formule particulièrement adaptée aux apprenants disposant déjà de connaissances préalables et ne nécessitant pas d'encadrement pédagogique.

Examen et Certification

Embarquement dans le Parcours d'Examen

Entamez l'étape clé du parcours de certification PECB grâce à des examens conçus pour évaluer vos capacités de raisonnement critique et de résolution de problèmes. Disponibles dans le monde entier par l'intermédiaire de partenaires et distributeurs agréés, les examens PECB sont proposés sous deux formats pratiques afin de répondre à vos besoins :

- **Examen sur papier**

Les épreuves sont remises aux candidats sous format papier. L'utilisation d'appareils électroniques tels que les ordinateurs portables, tablettes ou smartphones n'est pas autorisée. La session d'examen est supervisée par un surveillant agréé PECB, sur le site où le partenaire a organisé la formation.

- **Examen en ligne**

Les épreuves sont mises à disposition des candidats sous format électronique via l'application PECB Exams. L'utilisation d'appareils électroniques tels que les tablettes et smartphones n'est pas autorisée. La session d'examen est supervisée à distance par un surveillant en ligne agréé PECB, à l'aide de l'application PECB Exams et d'une caméra externe ou intégrée.

Types d'Examens PECB

➤ **QCM à livre fermé** : Les candidats ne sont pas autorisés à utiliser des documents de référence. Ce type d'examen est généralement utilisé pour les certifications Foundation **et** Transition**.**

➤ **Examen rédactionnel à livre ouvert :** Les candidats sont autorisés à utiliser les supports de référence suivants :

- Une copie papier de la norme principale
- Les supports de formation (accessibles via l'application **PECB Exams** et/ou imprimés)
- Les notes personnelles prises durant la formation (accessibles via l'application **PECB Exams** et/ou imprimées)
- Un dictionnaire papier

➤ **QCM à livre ouvert** : **Les candidats sont autorisés à utiliser les supports de référence suivants :**

- Une copie papier de la norme principale
- Les supports de formation (accessibles via l'application **PECB Exams** et/ou imprimés)
- Les notes personnelles prises durant la formation (accessibles via l'application **PECB Exams** et/ou imprimées)
- Un dictionnaire papier

Note importante :
Les examens rédactionnels à livre ouvert sont progressivement remplacés par des examens **QCM à livre ouvert**. Ces examens intègrent des questions basées sur des scénarios, permettant d'évaluer la capacité des candidats à **appliquer**, **analyser** et **évaluer** efficacement les informations.

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

Examens Foundation	1 heure
Examens Manager	2 heures
Examens Lead	3 heures
Examens Cybersécurité Technique	6 heures

Remarque : Les examens en ligne et les examens sur papier ont la **même durée**, conformément aux indications mentionnées ci-dessus.

Comment démarrer et participer à nos formations

Pour entamer le processus et vous inscrire à nos formations, vous pouvez :

➤ **Trouver un organisme de formation dans votre région** en consultant la page dédiée : **https://www.chartered-managers.com/pecb/fr**

➤ **Vous inscrire à une formation et à un examen PECB** auprès de **CHARTERED MANAGERS**

Application PECB Exams

PECB Exams est une plateforme de test en ligne fiable et sécurisée qui vous permet de passer vos examens depuis n'importe quel lieu, à votre convenance, à condition de respecter les exigences définies par PECB. Elle offre une solution conviviale et respectueuse de l'environnement aux candidats, avec notamment les fonctionnalités suivantes :

- **Une option flexible**
- **Une évaluation instantanée et précise avec des résultats plus rapides**
- **Un niveau accru de sécurité et de confidentialité**

PECB propose **trois formats d'examens** à travers son vaste réseau de partenaires et de formateurs certifiés :

🔷 **PECB Exams :** Destiné aux candidats passant des examens de certification en ligne à leur convenance, sous la surveillance d'invigiles en ligne de PECB.

🔷 **PECB Exams – ATC :** Destiné aux partenaires organisant des examens privés de certification en ligne dans leurs centres d'examen, sans webcams ni microphones externes, en utilisant des flux de caméras de sécurité pour garantir la conformité.

🔷 **PECB Exams – Technical :** Destiné aux candidats passant des examens techniques de certification en cybersécurité en ligne, avec surveillance par PECB et des opportunités de laboratoires pratiques pour les candidats **Lead Ethical Hacking**, via des machines virtuelles et le logiciel client **PECB X2GO**.

EN SAVOIR PLUS

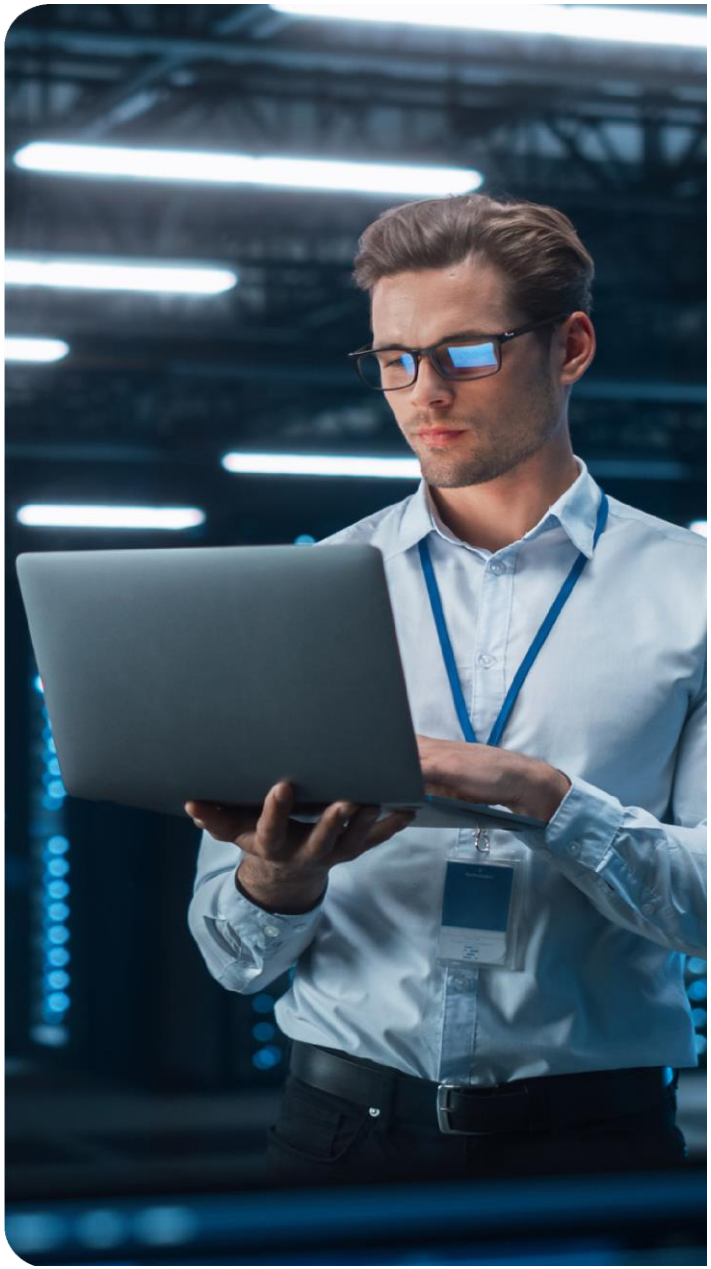
SECURITE DE L'INFORMATION

Pourquoi la sécurité de l'information ?

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

- **ISO/IEC 27001 -** Système de management de la sécurité de l'information
- **ISO/IEC 27002** - Contrôles de sécurité de l'information
- **CISO / RSSI -** Chief Information Security Officer ou Responsable de la sécurité des systèmes d'information
- **EBIOS -** Expression des Besoins et Identification des Objectifs de Sécurité
- **ISO/IEC 27005 -** Gestion des risques liés à la sécurité de l'information
- **ISO/IEC 27035 -** Gestion des incidents liés à la sécurité de l'information

Voir les formations en Sécurité de l'Information
https://chartered-managers.com/formations/securite-de-l-information/



ISO/IEC 27001 : Systèmes de Management de la Sécurité de l'Information

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

L'ISO / IEC 27001 spécifie les exigences relatives à l'établissement, la mise en œuvre, la mise à jour et l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. Ce cadre sert de guide pour réviser en permanence la sécurité de vos informations, ce qui sanctuarisera la fiabilité et ajoutera de la valeur à votre organisation.

L'ISO / IEC 27001 vous aide à comprendre les approches pratiques qui entrent en jeu dans la mise en œuvre d'un Système de management de la sécurité de l'information qui préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de management du risque. Par conséquent, la mise en œuvre d'un Système de management de la sécurité de l'information conforme à toutes les exigences de la norme ISO / IEC 27001 permet à vos organisations d'évaluer et de traiter les risques de sécurité de l'information auxquels elles sont confrontées.

Les personnes certifiées ISO / IEC 27001 démontrent qu'elles possèdent l'expertise nécessaire pour aider les organisations à mettre en œuvre des politiques et procédures de sécurité de l'information adaptées aux besoins de l'organisation

Avantages de la certification ISO/IEC 27001

1. Amélioration de la sécurité de l'information
2. Meilleure gestion des risques
3. Renforcement des compétences organisationnelles
4. Accès à un réseau mondial d'experts en normes de sécurité

En savoir plus ➔ **https://www.chartered-managers.com/pecb/iso-iec-27001**

Formation et objectifs d'apprentissage	Durée
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**

ISO/IEC 27002 : Contrôles de Sécurité de l'Information

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

L'ISO/IEC 27002 est une norme internationale qui définit les lignes directrices relatives aux bonnes pratiques de management de la sécurité de l'information. Ces pratiques de gestion aideront vos organisations à renforcer la confiance dans leurs activités inter organisationnelles et à mettre en place un ensemble approprié de mesures, y compris les politiques, les processus, les structures organisationnelles et les fonctions logicielles et matérielles. Cette norme est un document générique utilisé comme référence pour la sélection des mesures dans le cadre du processus de mise en œuvre du système de management de la sécurité de l'information. L'ISO/IEC 27002 est destinée à être utilisée par tous types d'organisations, les secteurs publics comme privé, les entreprises commerciales et celle à but non lucratif ainsi que toute autre organisation confrontée à des risques de sécurité de l'information.

La formation ISO/IEC 27002 est essentielle car elle vous fournira les lignes directrices fondamentales qui vous aideront à initier, à mettre en œuvre, à maintenir et à améliorer le management de la sécurité de l'information au sein d'une organisation. Les mesures de sécurité de l'information qui sont énumérées dans la norme sont conçues pour vous aider à identifier et à répondre aux exigences spécifiques dans une approche formelle d'appréciation des risques.

Les formations ISO/IEC 27002 vous permettront d'acquérir les connaissances nécessaires pour assurer aux organisations que leurs actifs informationnels précieux sont protégés par une norme internationale reconnue. Les avantages indiqués ci-dessus sont valables pour les organisations de tous niveaux de maturité de la sécurité et ne se limitent pas aux grandes organisations.

Avantages de la certification ISO/IEC 27002

1. Faire face aux cybermenaces émergentes
2. Renforcer l'assurance des données
3. Garantir la conformité réglementaire
4. Protéger les données sensibles

Formations et objectifs d'apprentissage	Durée
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	**5 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**

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27002

CISO - Chief Information Security Officer / RSSI - Responsable de la Sécurité de l'Information

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/RSSI

1. Évolution de carrière
2. Crédibilité et attractivité accrues sur le marché
3. Connaissances approfondies
4. Reconnaissance mondiale

En savoir plus ➔ https://www.chartered-managers.com/pecb/ciso/

Formations et objectifs d'apprentissage	Durée
Certified Information Security Officer (CISO/RSSI) Acquérir les connaissances, compétences et stratégies nécessaires pour diriger efficacement des programmes de sécurité de l'information	**5 JOURS**

➔➔ S'inscrire

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Présentation de PECB CISO et de son processus de certification

EBIOS est un outil d'appréciation des risques développé par le Service Central de la Sécurité des Systèmes d'Information (SCSSI) pour apprécier et traiter les risques au sein d'un système d'information. Bien qu'il puisse s'appliquer à différents domaines, EBIOS est principalement utilisé pour gérer les risques liés à la sécurité de l'information, les risques liés à la protection de la vie privée, les infrastructures critiques et l'ergonomie des outils de travail.

En tant qu'approche de management du risque, EBIOS permet d'identifier, d'analyser, d'apprécier et de traiter les risques dans le cadre d'une démarche d'amélioration continue. L'approche EBIOS adopte un cycle itératif qui s'articule autour de cinq phases, également appelées ateliers : cadrage et socle de sécurité, sources de risque, scénarios stratégiques, scénarios opérationnels et traitement du risque.

Les formations EBIOS de PECB fournissent un ensemble complet de guides dédiés au management des risques liés au système d'information. Elles vous permettent d'acquérir une approche cohérente et de haut niveau du traitement des risques.

En obtenant la certification PECB Certified EBIOS Risk Manager, vous serez à même de démontrer vos connaissances pratiques et vos capacités professionnelles à soutenir une organisation dans la réalisation et le suivi de ses analyses de risques.

Avantages de la certification CISO/RSSI

1. Évolution de carrière en sécurité de l'information
2. Contribution à une sécurité robuste
3. Reconnaissance de l'expertise
4. Engagement envers des normes de sécurité élevées

En savoir plus ➔ **https://www.chartered-managers.com/pecb/mar/**

Formations et objectifs d'apprentissage	Durée
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 : Gestion des Risques Liés Sécurité de l'Information

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

L'ISO / IEC 27005 fournit les lignes directrices pour l'établissement d'une approche systématique de la gestion des risques liés à la sécurité de l'information laquelle est nécessaire pour identifier les besoins organisationnels en matière de sécurité de l'information et pour créer un système efficace de management de la sécurité de l'information.

De plus, cette norme internationale vient en appui des concepts ISO/IEC 27001 et est conçue pour aider à la mise en œuvre efficace de la sécurité de l'information basée sur une approche de gestion des risques. La formation offerte par PECB vous aidera à aligner correctement le système de management de la sécurité de l'information des organisations avec le processus de gestion des risques liés à la sécurité de l'information.

De surcroit, une fois les certificats PECB Certified ISO/IEC 27005 obtenus, vous pourrez aider les organisations à améliorer continuellement leurs processus de gestion des risques liés à la sécurité de l'information ce qui assurera la réalisation des objectifs de l'organisation.

Avantages de la certification ISO/IEC 27005

1. Expertise dans la protection de l'information
2. Adaptabilité face à l'évolution du paysage de la sécurité
3. Décisions éclairées en matière de traitement des risques
4. Identification des menaces et des vulnérabilités

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27005

Formations et objectifs d'apprentissage	Durée
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**

ISO/IEC 27034 : Sécurité des Applications

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

1. Renforcement de l'expertise dans un domaine essentiel de la sécurité informatique
2. Perspectives de carrière de haut niveau en cybersécurité
3. Leadership stratégique
4. Développement professionnel

Formations et objectifs d'apprentissage	Durée
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**

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27034

ISO/IEC 27035 : Gestion des Incidents de Sécurité de l'Information

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

À une époque où les incidents de cybersécurité deviennent de plus en plus sophistiqués et omniprésents, la nécessité de disposer de cadres solides de gestion des incidents n'a jamais été aussi cruciale. La série ISO/CEI 27035 répond à cet impératif en fournissant des lignes directrices complètes pour établir, mettre en œuvre, maintenir et améliorer continuellement la gestion des incidents de sécurité de l'information au sein des organismes.

Les formations PECB ISO/IEC 27035 permettent aux individus d'acquérir les compétences nécessaires pour établir, gérer et affiner la gestion des incidents de sécurité de l'information au sein de leur organisme. Cette gestion proactive des cyberincidents minimise l'impact des violations et renforce la résilience d'un organisme contre les menaces futures.

Elle permet aux entreprises de maintenir la continuité et de préserver leur réputation dans un environnement où la sécurité numérique fait partie intégrante du succès opérationnel et concurrentiel.

Avantages de la certification ISO/IEC 27035

5. Réponse efficace aux incidents
6. Renforcement de la sécurité organisationnelle
7. Reconnaissance mondiale
8. Amélioration des compétences et des connaissances en TI

Formations et objectifs d'apprentissage	Durée
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 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 27035	**3 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**

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27035

ISO/IEC 27400 : Sécurité et confidentialité de l'Internet des Objets (IoT)

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 les risques associés.

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

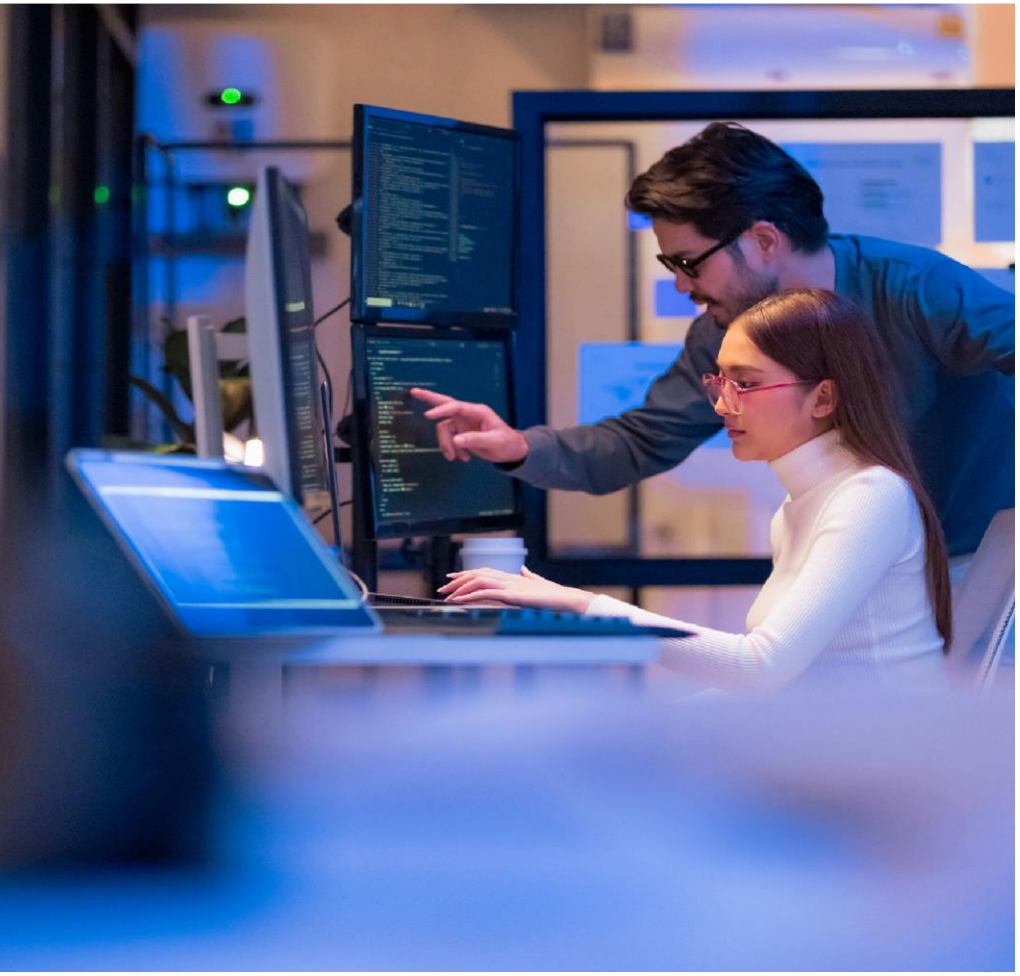
En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27400

Formations et objectifs d'apprentissage	Durée
ISO/IEC 27400 Foundation Acquérir des connaissances sur l'interprétation des lignes directrices d'ISO/IEC 27400 afin d'identifier, d'évaluer et de gérer les risques liés à la sécurité de l'information	**2 JOURS**
ISO/IEC 27400 Risk Manager	**3 JOURS**
ISO/IEC 27400 Lead Risk 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**

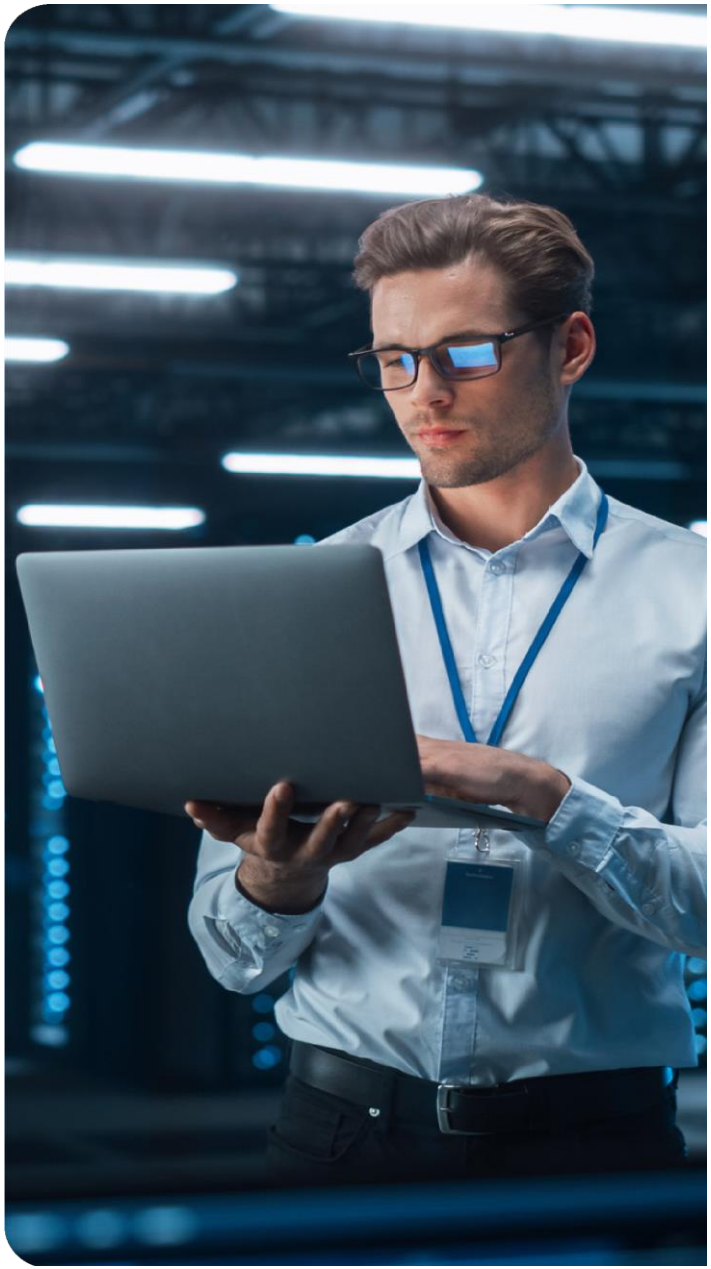
Responsable de la sécurité de l'information
Ce poste se concentre sur la gestion et la supervision de l'ensemble du programme de sécurité de l'information d'une organisation.
Salaire annuel moyen : **U.S. $187,221**

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.*

GESTION DE LA CYBERSECURITE



Pourquoi le management de la cybersécurité ?

Le management de la cybersécurité est indispensable car il fournit l'orientation stratégique et les mécanismes de contrôle nécessaires pour protéger les ressources numériques d'une organisation et assurer la continuité et la fluidité de ses opérations.

- Management de la Cybersécurité
- Cloud Security ou sécurité du cloud
- Penetration Testing ou Test d'intrusion
- SCADA Supervisory Control and Data Acquisition ou Système de contrôle et d'acquisition de données)
- ISO/IEC 27033 Network Security
- CMMC (Cybersecurity Maturity Model Certification)
- NIS 2 Directive
- SOC 2

Management de la Cybersécurité

Présentation du Management 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

Avantages de la certification en Management de la Cybersecurité

1. Renforcement de l'expertise en sécurité numérique
2. Amélioration des compétences en leadership
3. Meilleure prise de décision
4. Compréhension élargie de l'évaluation des risques

Formations et objectifs d'apprentissage	Durée
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**

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27032

Cloud Security

Présentation du Cloud Security 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 en Management de la Cybersecurité

1. Compétences spécialisées
2. Pertinence dans le domaine en pleine croissance de la sécurité du cloud
3. Amélioration de l'employabilité
4. Renforcement de la sécurité de l'emploi

En savoir plus ➔ https://www.chartered-managers.com/pecb/cloud-security

Formations et objectifs d'apprentissage	Durée
Lead Cloud Security Manager 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 (Test d'intrusion)

Présentation du Penetration Testing et de son processus de certification

Un test d'intrusion consiste à évaluer la sécurité d'une infrastructure informatique en essayant en toute sécurité d'exploiter les vulnérabilités qui peuvent exister dans les systèmes d'exploitation, les configurations inappropriées, les erreurs d'application ou le comportement des utilisateurs finaux.

Les tests d'intrusions sont une tentative de tester l'efficacité des mesures de sécurité et de découvrir tout exploit potentiel ou les backdoors qui peuvent être présents dans les systèmes informatiques ; par lesquels les pirates informatiques et les cybercriminels peuvent obtenir un accès non autorisé ou mener des activités malveillantes. En outre, le test d'intrusion est un outil avancé pour détecter, analyser et mettre en place des restrictions protectives à l'infrastructure informatique, afin de pallier aux possibilités de pertes financières générées par les activités malveillantes.

Les professionnels des tests d'intrusion peuvent découvrir différents aspects des cadres de cybersécurité dans les systèmes informatiques et fournir des solutions détaillées aux risques de cybersécurité. L'objectif d'un professionnel des tests d'intrusion et son intérêt à suivre la formation « Lead Pen Testing Professional » réside dans la maîtrise d'une méthode de test d'intrusion répétable et documentable qui peut être utilisée dans un test d'intrusion dans le cadre professionnel

Avantages de la certification en Penetration Testing

1. Engagement envers la cybersécurité
2. En savoir plus Potentiel de rémunération plus élevé
3. Développement professionnel
4. Démonstration de compétences en piratage et en identification des vulnérabilités

En savoir plus ➔ https://www.chartered-managers.com/pecb/pen-test

Formations et objectifs d'apprentissage	Durée
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 - Supervisory Control and Data Acquisition (Système de contrôle et d'acquisition de données)

Présentation du SCADA et de son processus de certification

SCADA - Supervisory Control and Data Acquisition (Système de contrôle et d'acquisition de données) est un système de cadre applicatif industriel qui comprend à la fois l'architecture matérielle et logicielle pour contrôler, surveiller et analyser un processus industriel. SCADA est un logiciel d'application qui permet aux gestionnaires, aux ingénieurs et aux opérateurs de l'industrie de superviser et de communiquer efficacement avec l'environnement de travail.

En tant que logiciel d'application, SCADA est conçu pour aider les experts de l'industrie à maintenir et à améliorer les processus industriels. Par conséquent, l'objectif de SCADA est de collecter des données en temps réel, de stocker, de traiter et de générer des rapports pour les processus industriels complexes. L'objectif de SCADA est de fournir aux professionnels des techniques Catalogue des formations 2026 pour choisir, planifier et concevoir des technologies pour améliorer les processus métier et autres services.

En outre, SCADA aidera les professionnels à apprendre les compétences requises essentielles pour planifier, diriger, exploiter et gérer un système de projet dans un environnement de travail. L'importance de SCADA réside dans système d'automatisation qui permet à l'organisation et aux professionnels d'anticiper les incertitudes liées au risque, de réduire les coûts d'investissement, de maintenance et d'étudier des réponses optimales à la continuité des processus industriels.

Avantages de la certification en SCADA

1. Amélioration de la mise en œuvre de la sécurité
2. En savoir plus Approche professionnelle globale de la sécurité
3. Renforcement des connaissances en sécurité SCADA
4. Approche holistique de la sécurité

Formations et objectifs d'apprentissage	Durée
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**

En savoir plus ➔ https://www.chartered-managers.com/pecb/scada/

ISO/IEC 27033 Network Security

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

La série de normes ISO/IEC 27033 comprend six parties conçues pour garantir la sécurité réseau des appareils, des applications, des services et des utilisateurs finaux. Elle couvre la sécurisation des communications entre les réseaux à l'aide de passerelles de sécurité, de réseaux privés virtuels (VPN) et d'accès sans fil aux réseaux IP.

La norme ISO/IEC 27033-1 est une cartographie des autres parties. Elle fournit une vue d'ensemble des concepts et des conseils de gestion en matière de sécurité des réseaux en aidant les organisations à identifier et à analyser les risques et les exigences en matière de sécurité des réseaux.

La norme ISO/IEC 27033-2 fournit des lignes directrices sur la planification, la conception, la mise en œuvre et la documentation de la sécurité des réseaux. Elle présente l'architecture de sécurité des réseaux, ses exigences et ses principes de conception. Catalogue des formations 2026 La norme ISO/IEC 27033-3 illustre des scénarios de réseau et les menaces qui y sont associées, les techniques de conception et les questions de contrôle. Elle aide les organisations à examiner l'architecture technique de sécurité, la conception et les contrôles de sécurité.

La norme ISO/IEC 27033-4 fournit des lignes directrices sur les risques, les techniques de conception et les contrôles des passerelles de sécurité. Elle présente des passerelles de sécurité pour sécuriser les flux d'informations entre les réseaux.

La norme ISO/IEC 27033-5 fournit des lignes directrices sur les risques, les techniques de conception et les contrôles des réseaux privés virtuels (VPN). Elle aide les organisations à sélectionner, mettre en œuvre et surveiller les contrôles techniques nécessaires pour connecter les utilisateurs distants aux réseaux.

La norme ISO/IEC 27033-6 fournit des lignes directrices sur les risques, les techniques de conception et les contrôles des réseaux sans fil IP. Elle aide les organisations à sélectionner, mettre en œuvre et surveiller les contrôles techniques nécessaires pour sécuriser les communications entre les réseaux sans fil. Cette partie présente les réseaux personnels sans fil (WPAN), les réseaux locaux sans fil (WLAN) et les réseaux métropolitains sans fil (WMAN)..

Avantages de la certification ISO/IEC 27077

1. Valorisation de la carrière en informatique et en cybersécurité
2. Préparation aux défis complexes
3. Crédibilité professionnelle renforcée
4. Meilleure attractivité sur le marché

En savoir plus
➔ https://www.chartered-managers.com/pecb/iso-iec-27033

Formations et objectifs d'apprentissage	Durée
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**

CMMC - Cybersecurity Maturity Model certification

Présentation du CMMC et de son processus de certification

Le cadre Cybersecurity Maturity Model Certification (CMMC) est un mécanisme de vérification conçu pour évaluer le niveau de maturité des organisations en matière de protection des informations non classifiées telles que les informations des contrats fédéraux (FCI) et les informations contrôlées non classifiées (CUI). Il s'agit d'un nouvel ensemble de normes sur la cybersécurité qui englobe diverses normes, références et autres bonnes pratiques en matière de cybersécurité. Il comprend un certain nombre de processus et de pratiques qui sont répartis sur cinq niveaux de certification cumulatifs.

Le modèle CMMC est développé et géré par le département de la Défense (DoD) et est considéré comme la réponse du DoD aux éventuels compromissions d'informations sensibles résidant sur les systèmes et réseaux de la base industrielle de la défense (DIB). Le CMMC-AB, quant à lui, est la seule source faisant autorité pour l'opérationnalisation des évaluations et de la formation CMMC.

Les formations CMMC vous aideront à acquérir des connaissances sur les domaines, pratiques et processus CMMC et à comprendre comment ils peuvent être appliqués dans la chaîne d'approvisionnement du DoD. En outre, ces formations vous aideront à comprendre le processus de certification CMMC et vous prépareront à votre rôle dans l'écosystème CMMC-AB.

Avantages de la certification CMMC

1. Connaissances avancées en cybersécurité
2. Expertise en conformité En savoir plus
3. Reconnaissance sectorielle
4. Évolution de carrière en cybersécurité

En savoir plus
➔ https://www.chartered-managers.com/pecb/cmmc

Formations et objectifs d'apprentissage	Durée
CMMC Foundation 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	**5 JOURS**

➔➔ **S'inscrire**

Directive NIS 2

Présentation de la Directive NIS2 et de son processus de certification

La directive NIS 2 (également connue sous le nom de directive (UE) 2022/2555) est entrée en vigueur le 16 janvier 2023 afin de renforcer la sécurité des réseaux et des systèmes d'information dans l'Union européenne. Cette directive vise spécifiquement les opérateurs d'infrastructures critiques et les fournisseurs de services essentiels, en imposant la mise en œuvre de mesures de cybersécurité robustes et le signalement rapide des incidents aux autorités compétentes.

Le champ d'application de la directive NIS 2 est plus large, englobant un plus grand nombre d'organismes et de secteurs, tout en renforçant les exigences en matière de sécurité, en simplifiant les obligations de déclaration et en imposant des mesures et des sanctions plus strictes. En adhérant aux exigences énoncées dans la directive NIS 2, les organismes peuvent renforcer leurs défenses en matière de cybersécurité, sauvegarder les Catalogue des formations 2026 actifs critiques et contribuer activement à la construction d'un environnement numérique sûr au sein de l'Union européenne.

Les personnes certifiées pour la directive NIS 2 démontreront leur compréhension approfondie des exigences de la directive, des stratégies de mise en œuvre et des bonnes pratiques pour protéger les infrastructures critiques contre les cybermenaces. Doté de ces connaissances, vous aurez la capacité de diriger les organismes dans la gestion efficace des cybermenaces et la mise en œuvre de contrôles appropriés, tout en assurant la conformité avec la directive NIS 2

Avantages de la certification NIS 2

1. Conformité aux normes de l'Union européenne
2. Engagement renforcé en matière de cybersécurité
3. Crédibilité accrue
4. Expertise dans les secteurs critiques

En savoir plus
➔ https://www.chartered-managers.com/pecb/nis-2-directive

Formations et objectifs d'apprentissage	Durée
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 - Systems and Organization Controls

Présentation de 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

1. Expertise en évaluation de la sécurité
2. Préparation pour responsabilités élevées
3. Compétences en résolution de problèmes
4. Positionnement professionnel renforcé en tant qu'expert en cybersécurité

En savoir plus
➔ https://www.chartered-managers.com/pecb/soc-2

Formations et objectifs d'apprentissage	Durée
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

1. Solutions de cybersécurité adaptées
2. Expertise en évaluation des menaces
3. Évolution de carrière
4. Connaissances approfondies en tant qu'expert en cybersécurité

En savoir plus
➔ https://www.chartered-managers.com/pecb/nist

Formations et objectifs d'apprentissage	Durée
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 – Systèmes d'Automatisation et de Contrôle Industriels

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

1. Compétences démontrées en cybersécurité industrielle
2. Amélioration de l'évaluation des fournisseurs et des prestataires de services
3. Capacité à réaliser des évaluations des risques IACS
4. Adaptation efficace des principes de sécurité informatique aux environnements OT
5. Compétence dans la conception de systèmes industriels sécurisés dès la conception
6. Amélioration de la communication entre les parties prenantes grâce à un langage de normes unifié
7. Capacité renforcée à maintenir et améliorer la sécurité des IACS

Formations et objectifs d'apprentissage	Durée
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**

8. Crédibilité professionnelle reconnue à l'échelle mondiale en matière de sécurité des IACS

En savoir plus ➔ https://www.chartered-managers.com/pecb/isa-iec-62443

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 lucratives dans le domaine de la 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**

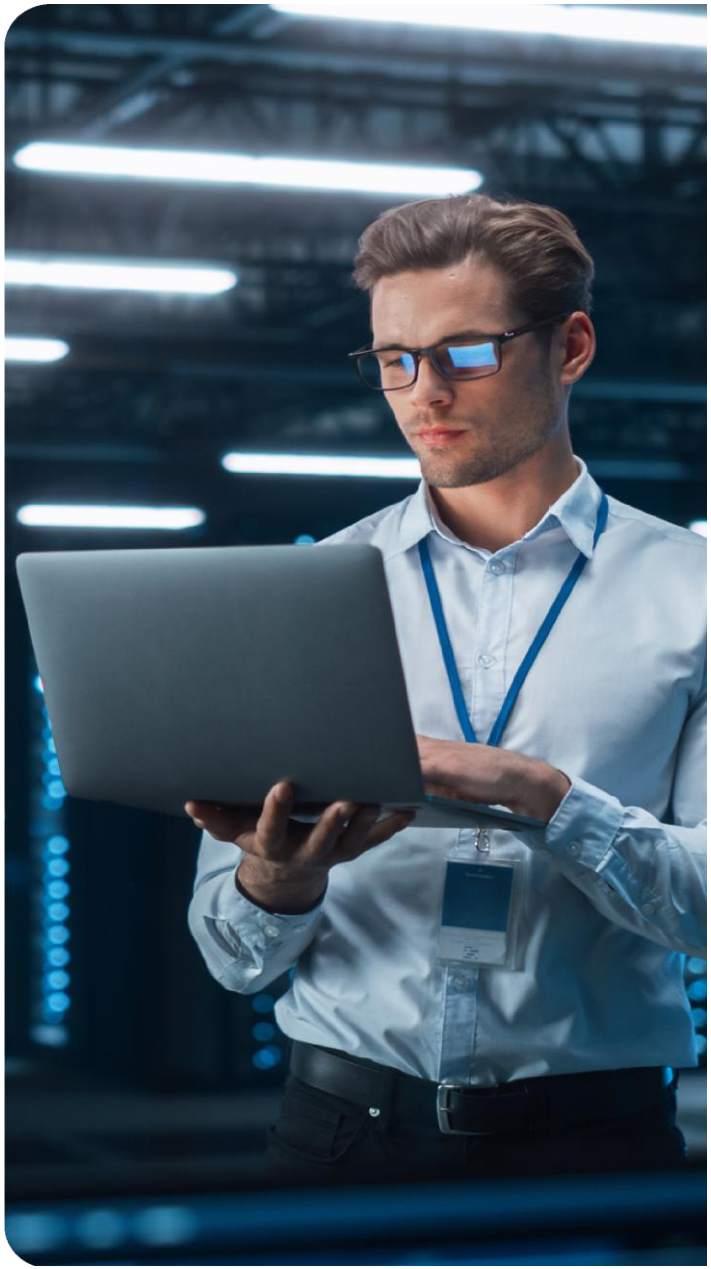
Testeur d'intrusion

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.*

CYBERSECURITE TECHNIQUE



Pourquoi la cybersécurité technique ?

La cybersécurité technique est cruciale car elle regroupe les outils, technologies et méthodes qui permettent de protéger activement les systèmes et les données contre les cybermenaces.

- Ethical Hacking (Piratage Ethique)
- Certified Cyber Threat Analyst (CCTA)
- Certified Digital Forensics Examiner (Enquêteur certifié en criminalistique numérique)
- Linux Foundations
- Certified Advanced Penetration Tester (CAPT)

Ethical Hacking (Piratage Ethique)

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

Le piratage éthique est l'acte de pénétrer dans des systèmes, réseaux ou applications informatiques dans le but d'exploiter des vulnérabilités qui peuvent conduire à des menaces et des risques potentiels. L'objectif principal du piratage éthique est d'améliorer la sécurité globale des organisations en comblant les écarts et les vulnérabilités découverts lors des tests d'intrusion. Les pirates éthiques sont autorisés à utiliser les mêmes techniques de piratage que les pirates malveillants, avec l'autorisation de l'organisation à tester.

Les hackers éthiques sont également connus sous le nom de « white hats hackers », car ils utilisent leur expertise en matière de piratage pour améliorer la sécurité des organisations en réduisant le nombre de vulnérabilités et de violations de la sécurité. Avec l'augmentation du nombre de cyberattaques, la demande mondiale de services de piratage éthique est en constante augmentation. Des organisations connues dans le monde entier ont choisi d'inclure le piratage éthique dans leurs stratégies de sécurité, augmentant ainsi la demande de pirates éthiques dans divers secteurs. En outre, les pirates éthiques expérimentés gagnent des salaires plus élevés que les autres professionnels. `

En tant que pirate éthique, vous prouverez que vous possédez l'expertise nécessaire pour aider les organisations à détecter leurs faiblesses, avant qu'un pirate « black hat » ne le fasse. De plus, vous serez en mesure de démontrer que vous disposez des compétences nécessaires pour soutenir le processus d'intégration des tests d'intrusion dans les processus de l'organisation et garantir que les résultats escomptés sont atteints.

Développez vos connaissances en matière de piratage éthique et de sécurité informatique ; améliorez vos compétences en matière de piratage et perfectionnez votre connaissance des techniques les plus avancées en matière de sécurité informatique.

Avantages de la certification CLEH

1. Renforcement des compétences en sécurité offensive
2. Expertise complète en piratage éthique
3. Maîtrise des techniques avancées de piratage éthique
4. Amélioration des capacités de résolution de problèmes

En savoir plus
➔ https://www.chartered-managers.com/pecb/ethical-hacking

Formations et objectifs d'apprentissage	Durée
Certified Lead Ethical Hacker 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**

CYBERSECURITE TECHNIQUE

Certified Cyber Threat Analyst (CCTA)

Présentation du CCTA et de son processus de certification

Un analyste des menaces est un professionnel de la cybersécurité spécialisé dans la détection, l'analyse et l'atténuation des cybermenaces. Ce rôle est essentiel pour protéger l'infrastructure numérique et les informations sensibles d'une organisation. Les principales activités d'un analyste des menaces comprennent l'analyse des menaces et la recherche des menaces. L'analyse des menaces consiste à examiner systématiquement les menaces potentielles afin d'identifier leur nature, leur origine et leur impact potentiel. Elle évalue les vulnérabilités, prédit les vecteurs d'attaque potentiels et évalue la gravité des menaces afin de fournir des renseignements exploitables. Parallèlement, la recherche de menaces est une approche proactive qui consiste à parcourir les réseaux et les ensembles de données afin d'identifier et d'atténuer les menaces avancées qui ont contourné les mesures de sécurité d'une organisation. Les chercheurs de menaces utilisent des outils et des techniques sophistiqués pour découvrir et minimiser les menaces cachées avant qu'elles ne causent des dommages importants.

En menant ces activités, un analyste des menaces aide les organisations à garder une longueur d'avance sur les cybermenaces, garantissant ainsi une défense solide contre les cyberattaques potentielles.

En tant que professionnel dans le domaine de la cybersécurité, l'obtention de la certification Certified Threat Analyst (CCTA) peut considérablement améliorer votre carrière. Cette certification vous permet d'acquérir les compétences et les connaissances essentielles pour identifier, analyser et atténuer efficacement les cybermenaces. Grâce à la certification CCTA, vous pouvez démontrer votre maîtrise des différents types de menaces et vecteurs d'attaque auxquels les organisations sont confrontées aujourd'hui. Cette capacité est cruciale pour aider les organisations à développer des mécanismes de défense robustes contre les cybermenaces

Avantages de la certification CCTA

1. Renforcement de la détection et de la réponse aux menaces
2. Chasse proactive aux menaces
3. Amélioration de la gestion des incidents
4. Adoption de cadres avancés

En savoir plus
➔ https://www.chartered-managers.com/pecb/ccta

Formations et objectifs d'apprentissage	Durée
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**

Certified Digital Forensics Examiner (Enquêteur certifié en criminalistique numérique)

Présentation de l'examinateur certifié en criminalistique numérique 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.

Avantages de la certification CDFE

1. Accès à des outils et techniques avancés d'informatique légale
2. En savoir plus Anticipation des menaces émergentes
3. Amélioration des capacités de réponse aux incidents
4. Connaissances pratiques des outils d'informatique légale

En savoir plus
➔ https://www.chartered-managers.com/pecb/digital-forensics/

Formations et objectifs d'apprentissage	Durée
Certified Digital Forensics 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

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 f ichiers, 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 Linux Foundations

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

En savoir plus
➔ https://www.chartered-managers.com/pecb/linux

Formations et objectifs d'apprentissage	Durée
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 (CAPT) 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

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

En savoir plus
➔ https://www.chartered-managers.com/pecb/capt

Formations et objectifs d'apprentissage	Durée
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**

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**

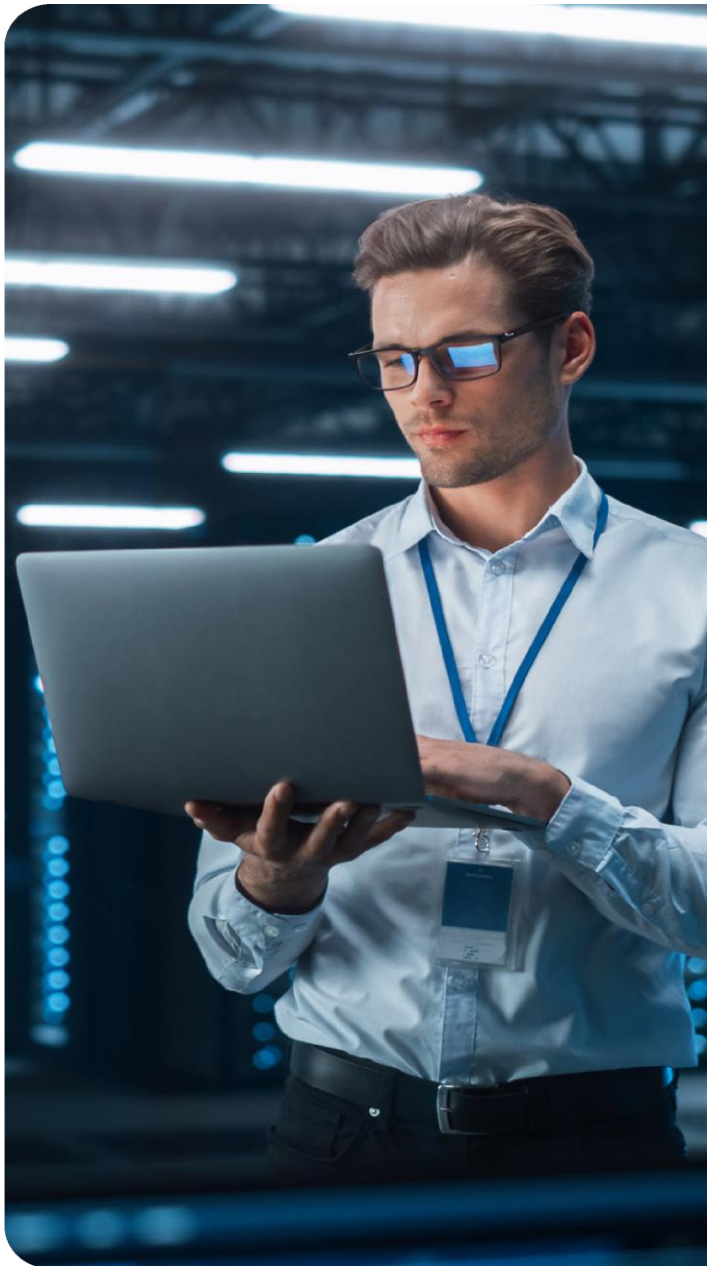
Certified Cloud Incident Responder (CCIR)
Intervient et gère les incidents de sécurité dans des environnements cloud, notamment les violations de données, les accès non autorisés, les infections par malwares et les erreurs de configuration.
Salaire annuel moyen : **U.S. $116,000**

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**

RESILIENCE, CONTINUITE ET REPRISE D'ACTIVITE



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 la capacité d'adaptation, assurent une reprise rapide et favorisent la confiance des parties prenantes, positionnant les organisations sur la voie d'un succès continu dans un environnement concurrentiel et imprévisible

ISO 22301 – Système de Management de la Continuité d'Activité

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

La norme ISO 22301 spécifie les exigences relatives aux systèmes de management de la continuité d'activité (SMCA), avec un cadre complet qui permet aux organismes d'anticiper les perturbations, de s'y préparer, d'y répondre et de s'en rétablir efficacement. Un SMCA efficace permet aux organismes de détecter et d'atténuer les menaces potentielles, pour garantir la continuité de leurs opérations.

La norme ISO 22301 fournit des exigences qui conviennent à tous les organismes, indépendamment de leur type, de leur taille et de la complexité de leurs opérations, ce qui leur permet d'adapter la norme à leurs environnements de fonctionnement uniques. La norme ISO 22301 est particulièrement utile pour les organismes qui cherchent à maintenir la prestation des services pendant les perturbations et à renforcer leur résilience globale.

La norme ISO 22301 sert à la fois de mécanisme de prévention et d'outil d'évaluation. À ce titre, elle aide les organismes à évaluer leur capacité à répondre à des besoins et obligations spécifiques en matière de continuité d'activité, ce qui contribue en fin de compte à la stabilité des opérations. Les professionnels certifiés ISO 22301 pourront démontrer leur connaissance des exigences de la norme, ainsi que des stratégies et compétences nécessaires pour une mise en œuvre efficace.

Cette certification offre aux personnes certifiées les connaissances nécessaires pour diriger des équipes dans la gestion efficace des perturbations, la mise en œuvre de mesures robustes et l'assurance de la conformité à la norme ISO 22301, renforçant ainsi leur capacité à relever les défis et conserver un avantage concurrentiel en cas d'incidents ou de crise

Avantages de la certification ISO 22301

1. Expertise professionnelle en planification de la continuité et de la résilience des activités
2. Opportunités de carrière
3. Validation de la capacité de préparation organisationnelle
4. Crédibilité renforcée en matière de continuité et de planification des activités

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-22301

Formations et objectifs d'apprentissage	Durée
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**

Disaster Recovery (Reprise d'Activité Après Sinistre)

Présentation de la Reprise d'Activité Après Sinistre et de son processus de certification

La reprise d'activité après sinistre comprend les politiques et les procédures visant à protéger une organisation contre les perturbations humaines ou naturelles de l'infrastructure informatique. Ils jouent un rôle considérable dans la prévention des pertes de données, des conséquences financières, de la perte de fiabilité et de la perte de réputation de l'organisation.

Un plan de secours ou de reprise des activités comprend les mesures qu'une organisation devrait prendre pour récupérer rapidement ses systèmes informatiques. Avoir l'expertise nécessaire pour soutenir une organisation dans la mise en œuvre, le maintien et la gestion d'un plan de reprise d'activité après sinistre vous garantit la reconnaissance professionnelle.

Acquérez les compétences essentielles et fondamentales en matière de reprise d'activité après sinistre et aidez votre organisation à développer des procédures, des plans et des processus de récupération. Être certifié en reprise d'activité après sinistre démontre votre détermination à atteindre un certain niveau de compétence professionnelle dans l'industrie.

Avantages de la certification en Reprise d'Activité Après Sinistre

1. Développement de compétences critiques
2. Validation de l'expertise en mise en œuvre de stratégies de reprise après sinistre
3. Protection des infrastructures
4. Opportunités de carrière

En savoir plus ➔ https://www.chartered-managers.com/pecb/disaster-recovery

Formations et objectifs d'apprentissage	Durée
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

Digital Operational Resilience Act (DORA)- Résilience opérationnelle numérique

Présentation de DORA et de son processus de certification

La résilience opérationnelle numérique désigne la capacité d'une entité financière à développer, garantir et réévaluer son intégrité opérationnelle d'un point de vue technologique en assurant directement ou indirectement, par le recours aux services de tiers prestataires de services informatiques, l'intégralité des capacités liées à l'informatique nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous tendent la fourniture continue de services financiers et leur qualité.

Alors que le secteur financier repose largement sur les technologies numériques, de nouvelles cybermenaces ne cessent de voir le jour. En réponse, l'Union européenne a élaboré la loi sur la Résilience opérationnelle numérique (DORA) pour améliorer la résilience opérationnelle du secteur financier.

DORA est la réglementation qui exige des entités du secteur f inancier de s'assurer qu'elles peuvent résister, répondre et se rétablir face à tous les types d'incidents, de risques et de menaces liés aux TIC. Elle a été adoptée par le Parlement européen et le Conseil de l'Union européenne le 14 décembre 2022, Règlement (UE) 2022/2554, et vise à harmoniser et rationaliser les règlements liés à la gestions des risques liés aux TIC, afin d'assurer leur cohérence partout dans l'UE. DORA exige des entités financières d'adhérer au principe de proportionnalité, qui prend en compte la taille des opérations, le profil de risques et la complexité.

La formation PECB Certified DORA Lead Manager vous aidera à obtenir les connaissances et améliorer vos compétences pour l'établissement, la mise en œuvre et la gestion d'un cadre de gestion des risques liés aux TIC, conformément aux exigences de DORA. Les experts de PECB sont impatients de vous guider et de vous aider dans le processus de certification afin de vous faire vivre une expérience enrichissante.

Avantages de la certification DORA

1. Amélioration des perspectives de carrière
2. Capacité à naviguer dans des réglementations complexes
3. Avantage concurrentiel
4. Évolution de carrière

En savoir plus
➔ https://www.chartered-managers.com/pecb/dora

Formations et objectifs d'apprentissage	Durée
DORA Foundation Comprendre les éléments fondamentaux du Digital Operational Resilience Act	**2 JOURS**
Lead DORA Manager Maîtriser les compétences pour conduire la résilience numérique dans les entités financières et assurer la conformité avec DORA	**5 JOURS**

➔➔ **S'inscrire**

Gestion de Crise

Présentation de la Gestion de Crise et de son processus de certification

Imaginez que votre organisme subisse un événement causant des dommages irréparables et que vous réalisiez que la situation aurait pu être évitée ou mieux gérée. Très souvent, les organismes peuvent éviter une crise en gérant les situations et incidents mineurs en temps opportun. Ils peuvent également atténuer les effets d'une crise, même s'il n'est pas possible de l'empêcher de survenir. Cela peut se faire en mettant en œuvre des processus et des procédures pour prévenir les crises, s'y préparer et y répondre, ce que constitue la gestion de crise.

Une crise est un événement qui menace la continuité des opérations d'un organisme et peut aller jusqu'à provoquer son effondrement. Ces événements peuvent avoir des causes naturelles ou peuvent être d'origine humaine, et sont, entre autres, les catastrophes naturelles, les problèmes environnementaux, le terrorisme, les atteintes à la cybersécurité et l'inconduite des employés. Une crise peut apparaître subitement ou elle peut naître de petits incidents qui n'ont pas été traités ou qui ont été gérés de manière inappropriée.

En améliorant leur capacité en gestion de crise, les organismes peuvent non seulement se préparer pour les crises et les prévenir, mais elles peuvent également les gérer plus efficacement et en tirer des enseignements, en identifiant des opportunités d'amélioration. Les lignes directrices de la norme ISO 22361 peuvent aider tout organisme, indépendamment de son type, de sa taille et de son secteur, à identifier et à gérer les crises. La norme s'adresse particulièrement aux membres de la direction générale des organismes ayant des responsabilités stratégiques dans la mise en place et l'amélioration d'une capacité de gestion de crise, ainsi qu'aux personnes travaillant sous leur supervision.

Nos certifications en gestion de crise démontrent que vous êtes capable de concevoir, d'élaborer, de mettre en œuvre, de surveiller et d'améliorer de façon continue la capacité de gestion de crise d'un organisme. Si vous souhaitez apprendre les concepts et principes de la gestion de crise et savoir comment construire une capacité de gestion de crise avec succès, les formations de PECB répondront à vos besoins. Nous vous accompagnerons tout au long du processus pour vous offrir une expérience enrichissante.

Avantages de la certification en Gestion de Crise

1. Compétences en atténuation des crises
2. Expertise en communication de crise
3. Amélioration du leadership et de la prise de décision
4. Amélioration des perspectives de carrière

En savoir plus
➔ https://www.chartered-managers.com/pecb/crisis

Formations et objectifs d'apprentissage	Durée
Lead Crisis Manager Obtenez les compétences et les connaissances pour planifier, mettre en œuvre, gérer et améliorer une capacité de gestion de crise en vous basant sur les lignes directrices de la norme ISO 22361 et les meilleures pratiques en matière de gestion de crise.	**5 JOURS**

➔➔ **S'inscrire**

Gestion de la Résilience Opérationnelle

Présentation de la Résilience Opérationnelle et de son processus de certification

La résilience opérationnelle est la capacité d'une organisation à anticiper, se préparer, réagir et se remettre de perturbations imprévues tout en maintenant ses services essentiels. Le maintien et l'amélioration de la résilience impliquent de développer de manière proactive la capacité à absorber les incidents et à s'adapter aux changements. La résilience opérationnelle couvre les initiatives qui améliorent la gestion de la continuité des activités en se concentrant sur les impacts, l'appétit pour le risque et les niveaux de tolérance en cas de perturbations dans la fourniture de produits ou de services.

La gestion de la résilience opérationnelle est devenue cruciale pour les organisations en raison de la multiplication des événements perturbateurs, tels que les catastrophes naturelles, les événements géopolitiques, les défaillances technologiques ou d'autres crises imprévues. Les perturbations opérationnelles et l'indisponibilité des services commerciaux essentiels peuvent causer un préjudice important aux consommateurs, compromettre l'intégrité du marché et menacer la viabilité des organisations. La gestion de la résilience opérationnelle permet aux organisations de se protéger contre ces risques et de les exploiter comme des opportunités de croissance.

En fin de compte, la résilience permet aux organisations de se remettre rapidement des difficultés, de maintenir leur continuité et d'atteindre une croissance durable dans un environnement en constante évolution. En favorisant une culture qui valorise l'adaptabilité et l'amélioration continue, les organisations peuvent mieux répondre aux changements dans les attentes des clients, les modèles de demande et les structures industrielles. Cette transformation améliore l'efficacité opérationnelle et renforce la valeur financière et culturelle, ce qui génère un avantage stratégique à long terme. Nos certifications en matière de résilience opérationnelle démontrent votre capacité à planifier, gérer et améliorer en permanence la résilience opérationnelle de manière réfléchie.

Avantages de la certification en Résilience Opérationnelle

1. Maîtrise des mesures de résilience
2. Crédibilité professionnelle accrue
3. Ensemble de compétences à forte valeur ajoutée
4. Renforcement de la sécurité organisationnelle

En savoir plus
➔ https://www.chartered-managers.com/pecb/operational-resilience

Formations et objectifs d'apprentissage	Durée
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**

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 lucratives dans le domaine de la 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 : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

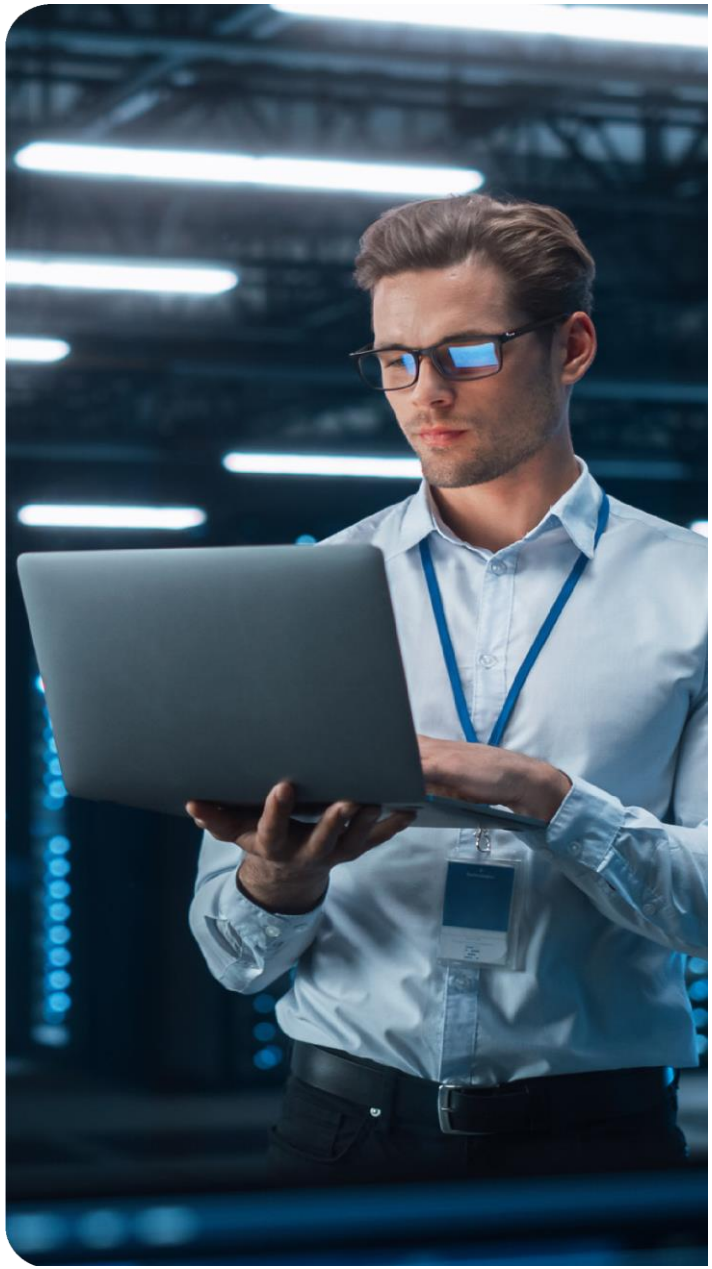
CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

Pourquoi la confidentialité et la protection des données ?

La confidentialité et la protection des données sont très importantes pour sécuriser les informations sensibles, garantir le respect des lois et renforcer la confiance des clients.

Elles contribuent à atténuer les risques de violations et de pertes financières, à soutenir la continuité des activités et à renforcer la résilience face aux cybermenaces constantes. Dans le monde numérique actuel, elles sont essentielles pour maintenir la sécurité, la confiance et la conformité légale.

- ISO/IEC 27701 - Système de gestion informations confidentielles
- RGPD – Règlement Général sur la Protection des Données



ISO/IEC 27701 - Système de gestion informations confidentielles

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

La norme ISO/IEC 27701 est publiée en août 2019 et c'est la première norme internationale qui traite du management de la protection de la vie privée. La norme aidera les organismes à établir, à tenir à jour et à améliorer continuellement un système de management en matière de protection de la vie privée (SMVP) en améliorant le SMSI existant, conformément aux exigences de la norme ISO/ IEC 27001 et aux orientations de la norme ISO/IEC 27002.

Il peut être utilisé par tous les types d'organismes, quels que soient leur taille, leur complexité ou le pays dans lequel ils opèrent. Cette norme est essentielle pour chaque organisation responsable des informations d'identification personnelle (IIP), car elle définit les exigences en matière de gestion et de traitement des données et de protection de la confidentialité. Elle enrichit un SMSI déjà mis en œuvre pour traiter correctement les problèmes de confidentialité en aidant les organisations à comprendre les approches pratiques impliquées dans la mise en œuvre d'une gestion efficace des IIP.

Souhaitez-vous approfondir vos connaissances et développer vos compétences en matière d'établissement, de mise en œuvre, de maintenance et d'amélioration d'un système de management de la protection de la vie privée ? Les experts PECB sont là pour faciliter le processus de certification et vous aider à obtenir la certification PECB Certified ISO/IEC 27701

Avantages de la certification ISO/IEC 27701

1. Renforcement du positionnement professionnel
2. Validation de l'expertise en management et en protection des données à caractère personnel
3. Portée mondiale
4. Opportunités d'évolution de carrière

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-27701

Formations et objectifs d'apprentissage	Durée
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**

➔➔ **S'inscrire**

RGPD – Règlement Général sur la Protection des Données

Présentation du RGPD et de son processus de certification

Le RGPD (ou GDPR) est le Règlement Général sur la Protection des Données (ou General Data Protection Regulation), une nouvelle réglementation européenne qui vise à renforcer le régime de protection des données pour les organismes qui opèrent dans l'Union européenne (UE) et qui traitent les données à caractère personnel des résidents européens.

Le RGPD consiste donc en la protection des données personnelles des employés, clients et autres. Par le même, il introduit une obligation de notification pour les organismes ayant à faire avec le traitement des données personnelles. En cas de non-conformité à ce règlement, ces organismes seront passibles de lourdes amendes et d'une réputation compromise. Considérant que les données personnelles représentent des informations critiques et sensibles que tous les organismes doivent protéger, une telle réglementation sera d'aide pour la mise en place des procédures et des contrôles appropriés afin de prévenir les violations de la sécurité de l'information.

Devenir un Data Protection Officer certifié vous permettra d'acquérir l'expertise nécessaire pour comprendre les risques qui pourraient avoir un impact négatif sur votre organisme et mettre en œuvre les réponses stratégiques requises sur la base des meilleures pratiques, exigences et principes du RGPD. La première étape vise à vous doter des principes fondamentaux de RGPD qui vous aideront à atteindre la conformité. Nos cours de formation sont dispensés par des formateurs expérimentés qui vous aideront à comprendre les concepts et les méthodes ainsi que la manière dont ils peuvent être applicables à votre organisme

Avantages de la certification RGPD

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

En savoir plus ➔ https://www.chartered-managers.com/pecb/gdpr

Formations et objectifs d'apprentissage	Durée
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**
Certification des Compétences du DPO (CNIL) Validez vos compétences en tant que DPO avec la certification PECB selon les exigences de la CNIL	**5 JOURS**

➔➔ **S'inscrire**

Pourquoi choisir une carrière dans le domaine de la confidentialité et de la protection des données ?

- ✓ Essentiel pour la protection des informations personnelles et sensibles
- ✓ Un domaine en pleine expansion grâce aux progrès technologiques
- ✓ Très gratifiant et ayant un impact significatif sur les entreprises et la société

Carrières lucratives dans le domaine de la confidentialité et de la protection des données

Responsable de la protection de la vie privée (CPO)
Poste de cadre supérieur chargé d'élaborer et de mettre en œuvre des politiques et des pratiques en matière de confidentialité, de garantir le respect des lois sur la protection des données et de gérer les risques liés à la confidentialité des données.
Salaire annuel moyen : **186 537 $ US**

Conseiller en confidentialité
Fournit une expertise juridique en matière de confidentialité et de protection des données, donne des conseils sur la conformité aux lois sur la confidentialité et traite les questions juridiques liées à la confidentialité. Salaire annuel moyen : **158 677 $ US**

Responsable du programme de confidentialité
Gère l'élaboration et la mise en œuvre de programmes de confidentialité, y compris les politiques, les formations et les initiatives de conformité. Salaire annuel moyen : **148 438 $ US**

Délégué à la protection des données (DPO)
Spécialisé dans la supervision de la stratégie et de la mise en œuvre de la protection des données afin d'assurer la conformité avec RGPD et d'autres lois sur la protection des données.
Salaire annuel moyen : **112 376 $ US**

Ingénieur en confidentialité
Développe et met en œuvre des solutions techniques et des contrôles pour garantir la confidentialité des données personnelles dans les systèmes et applications informatiques.
Salaire annuel moyen : **119 062 $ US**

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

INTELLIGENCE ARTIFICIELLE

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.

- ISO/IEC 42001, Système de management de l'intelligence artificielle
- CAIP - Artificial Intelligence Professional
- CAIM Artificial Intelligence Manager
- AI Risk Management
- CAIA – Artificial Intelligence Auditor

ISO/IEC 42001 – Management de l'Intelligence Artificielle

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

Alors que le monde assiste aux progrès incessants de l'intelligence artificielle (IA), le besoin d'une normalisation et d'une réglementation efficaces se fait de plus en plus sentir pour garantir son utilisation responsable. La norme ISO/IEC 42001 a été élaborée pour répondre aux demandes urgentes liées à l'expansion incontrôlée de l'IA et à ses menaces potentielles. Elle spécifie les exigences et offre des conseils pour établir, mettre en œuvre, maintenir et améliorer en permanence un système de management de l'IA (SMIA) dans le contexte d'une organisation. Elle fournit un cadre pour la mise en œuvre éthique des systèmes d'IA, en proposant une approche globale pour s'assurer que les technologies qui reposent sur cette intelligence respectent les principes d'équité, de transparence, de responsabilité et de respect de la vie privée.

Les formations PECB ISO/IEC 42001 permettent aux individus d'acquérir les compétences nécessaires pour planifier, développer, mettre en œuvre, maintenir et améliorer un système de management de l'IA au sein des organisations. Un SMIA efficace permet aux organisations d'utiliser tout le potentiel de l'IA à une époque où l'adaptation technologique est synonyme de progrès et de réussite. En outre, il aide les organisations à conserver un avantage concurrentiel dans un environnement technologique et commercial en constante évolution.

Avantages de la certification ISO/IEC 42001

1. Gestion efficace de l'IA
2. Crédibilité renforcée
3. Expertise spécialisée
4. Évolution de carrière

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-42001

Formations et objectifs d'apprentissage	Durée
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 reconnu	**5 JOURS**

➔➔ **S'inscrire**

CAIP – Professionnel Certifié en Intelligence Artificielle

Présentation de la norme CAIP et de son processus de certification

Alors que le monde assiste aux progrès incessants de l'intelligence artificielle (IA), le besoin d'une normalisation et d'une réglementation efficaces se fait de plus en plus sentir pour garantir son utilisation responsable. La norme CAIP a été élaborée pour répondre aux demandes urgentes liées à l'expansion incontrôlée de l'IA et à ses menaces potentielles. Elle spécifie les exigences et offre des conseils pour établir, mettre en œuvre, maintenir et améliorer en permanence un système de management de l'IA (SMIA) dans le contexte d'une organisation. Elle fournit un cadre pour la mise en œuvre éthique des systèmes d'IA, en proposant une approche globale pour s'assurer que les technologies qui reposent sur cette intelligence respectent les principes d'équité, de transparence, de responsabilité et de respect de la vie privée.

Les formations PECB CAIP permettent aux individus d'acquérir les compétences nécessaires pour planifier, développer, mettre en œuvre, maintenir et améliorer un système de management de l'IA au sein des organisations.

Un SMIA efficace permet aux organisations d'utiliser tout le potentiel de l'IA à une époque où l'adaptation technologique est synonyme de progrès et de réussite. En outre, il aide les organisations à conserver un avantage concurrentiel dans un environnement technologique et commercial en constante évolution.

Avantages de la certification Professionnel Certifié en Intelligence Artificielle (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 ➔ https://www.chartered-managers.com/pecb/caip

Formations et objectifs d'apprentissage	Durée
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.	**5 JOURS**

➔➔ **S'inscrire**

INTELLIGENCE ARTIFICIELLE

CAIM – Manager Certifié en Intelligence Artificielle – Certified AI Manager

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 Manager Certifié en Intelligence Artificielle (CAIM)

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

En savoir plus ➔ https://www.chartered-managers.com/pecb/caim

Formations et objectifs d'apprentissage	Durée
Certified Artificial Intelligence Manager (CAIM) 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	**5 JOURS**

➔➔ **S'inscrire**

INTELLIGENCE ARTIFICIELLE

Artificial Intelligence Risk Management

Présentation de la Gestion des Risques Liés à l'IA et de son processus de certification

La gestion des risques liés à l'IA est le processus systématique d'identification, d'évaluation, d'atténuation et de surveillance des risques liés aux technologies d'intelligence artificielle (IA). L'objectif est de réduire les conséquences négatives potentielles tout en maximisant les avantages de l'IA, en veillant à ce que les systèmes d'IA restent sécurisés, éthiques et conformes aux normes réglementaires.

Contrairement aux méthodes traditionnelles de gestion des risques qui s'appuient souvent sur des données historiques et des analyses manuelles, la gestion des risques basée sur l'IA peut s'adapter de manière dynamique en temps réel, à l'aide d'outils avancés tels que l'apprentissage automatique et l'analyse de données. Cette approche aide les organisations à identifier, évaluer et traiter les risques de manière efficace et précise.

Les organisations mettent en œuvre des cadres structurés Catalogue des formations 2026 de gestion des risques liés à l'IA afin d'établir des politiques, des procédures et des responsabilités claires tout au long du cycle de vie de l'IA. Ces cadres garantissent que les systèmes d'IA sont développés et maintenus de manière responsable, éthique et conforme aux normes réglementaires.

L'obtention d'une certification en gestion des risques liés à l'IA valide l'expertise en matière de conformité réglementaire, de pratiques éthiques en matière d'IA et de normes de gouvernance. Les professionnels certifiés améliorent non seulement leurs perspectives de carrière, mais se positionnent également comme des experts de confiance, aidant les organisations à adopter des solutions d'IA de manière responsable et sécurisée dans un paysage technologique en rapide évolution.

Avantages de la certification Lead AI Risk Manager

1. Compétence vérifiée en évaluation et supervision des risques liés à l'IA
2. Amélioration de la fiabilité
3. Renforcement de la confiance organisationnelle dans une IA responsable et conforme des performances des modèles d'IA
4. Supervision renforcée sur l'ensemble du cycle de vie de l'IA
   Amélioration de la capacité de l'organisation à adopter des solutions d'IA
5. Piloter des initiatives d'automatisation de l'IA responsables, conciliant innovation et gestion des risques

En savoir plus ➔ https://www.chartered-managers.com/pecb/ai-risk

Formations et objectifs d'apprentissage	Durée
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**

CAIA – Certified Artificial Intelligence Auditor

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 du CAIA

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

En savoir plus ➔ https://www.chartered-managers.com/pecb/caia

Formations et objectifs d'apprentissage	Durée
Certified Artificial Intelligence Auditor (CAIA) 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**

➔➔ **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 lucratives en Intelligence Artificielle (IA)

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**

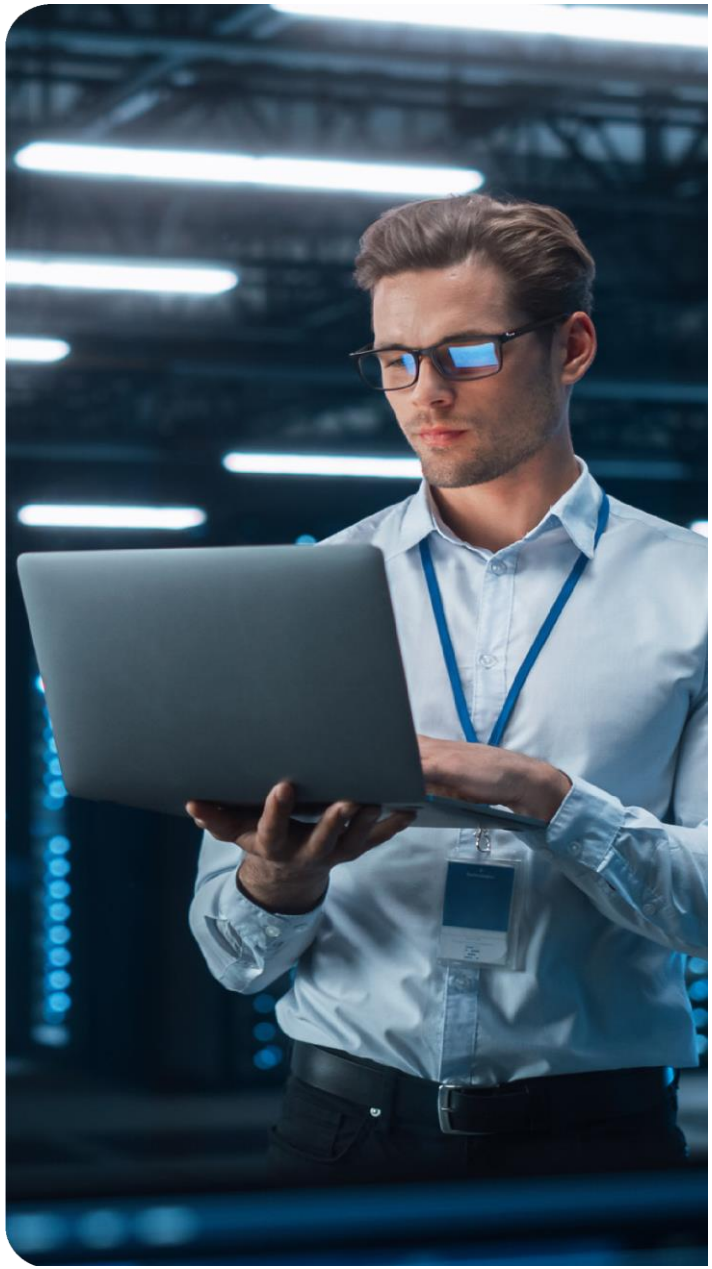
Remarque : *Les données salariales présentées ici proviennent de Glassdoor et peuvent évoluer au fil du temps en fonction de divers facteurs.*

TRANSFORMATION DIGITALE

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.

- Certified Digital Transformation Officer



Responsable certifié de la Transformation Digitale (CDTO)

Présentation du CDTO et de son processus de certification

La transformation numérique a permis à des organismes de différents secteurs d'atteindre une croissance et une productivité à long terme. Une stratégie de transformation numérique efficace permet d'éviter les problèmes potentiels pendant la transition numérique et après sa mise en œuvre. Une transformation numérique réussie nécessite une technologie appropriée et des personnes compétentes. Un responsable de transformation numérique est ainsi essentiel à la transformation numérique d'un organisme.

Les formations Certified Digital Transformation Officer sont adaptées à toute personne travaillant ou cherchant à travailler dans un domaine lié à la transformation numérique. Un CDTO (Certified Digital Transformation Officer) est une personne compétente dans l'utilisation, la mise en œuvre et le management des technologies de transformation numérique telles que la blockchain, l'intelligence artificielle, le big data, le cloud computing et l'Internet des objets (IoT).

La plupart des secteurs d'activité ont déjà entamé leur transformation numérique, celle-ci offrant agilité, flexibilité et croissance accélérée. L'adoption rapide de la transformation numérique nécessite le rôle d'un responsable de la transformation numérique.

En devenant un responsable certifié de transformation numérique (CDTO), vous allez pouvoir vous familiariser avec une feuille de route de transformation numérique et acquérir des connaissances tangibles sur les technologies émergentes qui permettent de répondre à l'évolution des besoins des entreprises et d'élargir le paysage de l'innovation numérique.

Avantages de la certification Digital Transformation Officer (CDTO)

1. Opportunités de réseautage
2. Leadership en stratégie numérique
3. Profil professionnel renforcé
4. Compétences tournées vers l'avenir

En savoir plus ➔ https://www.chartered-managers.com/pecb/digital-transformation/

Formations et objectifs d'apprentissage	Durée
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 lucratives 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**

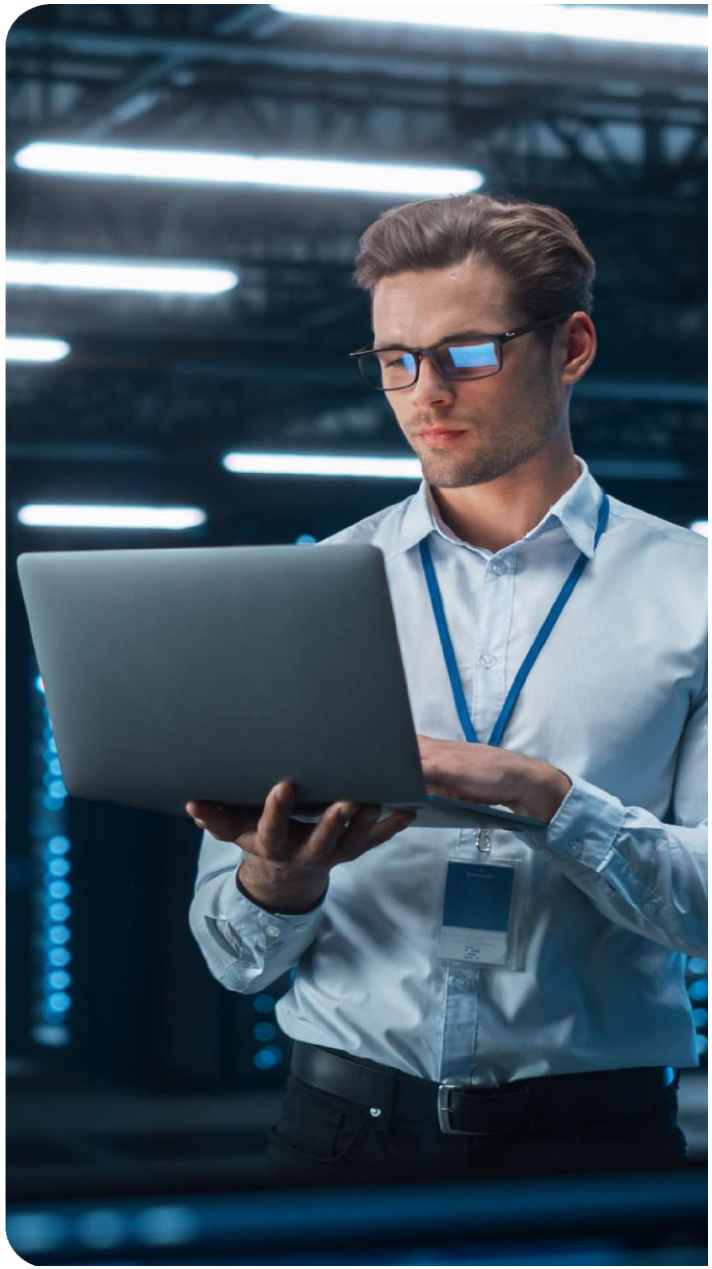
Enterprise Digital Architect
Conçoit des architectures numériques et technologiques à l'échelle de l'entreprise afin de soutenir les objectifs de transformation à long terme. Salaire annuel moyen : **U.S. $155,000**

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.*

GOUVERNANCE, RISQUE, CONFORMITE



Pourquoi la gouvernance, les risques et la conformité ?

La gouvernance, le risque et la conformité (GRC) aident les organisations à atteindre leurs objectifs tout en respectant les normes éthiques, réglementaires.
Elle garantit la responsabilité, gère Elle légales garantit et la les risques en continu et favorise une culture de conformité, réduisant ainsi les problèmes juridiques et renforçant la confiance des parties prenantes.
La GRC permet des opérations efficaces, responsables et durables dans un environnement commercial complexe.

- ISO 31000, Système de management des risques
- ISO 37000, Gouvernance des Organisations
- ISO 37001, Système de management anti-corruption
- ISO 37301 :2021, Système de management de la conformité-
- ISO/IEC 38500, Gouvernance des technologies de l'information par l'entreprise
- Certified Management Systems Internal Auditor (CMSIA

ISO 31000 – Systèmes de Management du Risque

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

L'ISO 31000 fournit des principes et des lignes directrices pour le management des risques afin d'identifier, d'apprécier et d'atténuer les risques auxquels sont confrontés les organismes. Elle recommande aux organismes de développer, mettre en œuvre et continuellement améliorer un cadre organisationnel qui vise à intégrer les processus de management des risques dans la gouvernance, la stratégie et la planification, la gestion, les processus d'élaboration des rapports, les politiques, les valeurs et la culture de l'organisme. Ce cadre organisationnel peut être utilisé indépendamment des types de risques et de l'organisme en question ; il aidera les organismes à protéger leur stabilité financière et leur réputation.

La norme ISO 31000 vous guidera vers l'identification des risques potentiels qui pourraient compromettre la réalisation d'objectifs cruciaux ; elle vous aidera à déterminer quels risques sont essentiels à prendre pour atteindre les objectifs primaires avant que les risques affectent les activités opérationnelles tout en gardant les autres risques sous contrôle..

Avantages de la certification ISO 31000

1. Renforcement des capacités professionnelles
2. Valeur stratégique
3. Renforcement des compétences en management du risque
4. Évolution de carrière

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-31000

Formations et objectifs d'apprentissage	Durée
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 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 Gouvernance informatique

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

La norme ISO/IEC 38500 fournit des principes, des définitions et un modèle de bonne gouvernance pour aider les dirigeants d'entreprises à cerner l'importance de la technologie de l'information (TIC). Cette norme vise à aider tous les types d'organisations à apprécier, diriger et surveiller l'utilisation des technologies de l'information peu importe le degré d'utilisation de celles-ci. Elle comporte des pratiques de management et de prise de décision associées à l'utilisation actuelle et future des technologies de l'information.

L'objectif visé par la norme est de favoriser l'efficacité, la rentabilité et la conformité de l'informatique dans toutes les entreprises en donnant aux dirigeants d'entreprises des informations et des orientations sur les modalités de la gouvernance informatique, et en établissant un vocabulaire de gouvernance informatique.

La norme ISO/IEC 38500 aide les dirigeants d'entreprises à veiller à ce que l'utilisation des TIC contribue positivement à la performance de l'organisation. Par conséquent, en satisfaisant aux exigences de l'ISO/IEC 38500, les organisations sont en mesure de surveiller l'utilisation des TIC, assurer la continuité des activités et leur viabilité, aligner les TIC sur les besoins de l'entreprise et assurer une mise en œuvre et un fonctionnement appropriés des actifs informatiques

Avantages de la certification ISO/IEC 38500

1. Gouvernance efficace des TI
2. Influence sur la stratégie informatique de l'organisation
3. Développement professionnel
4. Engagement envers les normes de gouvernance des TI

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-iec-38500

Formations et objectifs d'apprentissage	Durée
ISO/IEC 38500 Foundation Acquérir des connaissances sur les principaux composants de la norme ISO/IEC 38500, ses principes et ses approches en matière de management du risque	**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**

GOUVERNANCE, RISQUES, CONFORMITE

ISO 37000 Gouvernance d’entreprise

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

1. Maîtrise des pratiques de gouvernance
2. Prise de décision éthique
3. Renforcement de la confiance des parties prenantes
4. Opportunités de leadership

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-37000

Formations et objectifs d’apprentissage	Durée
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	**3 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**

GOUVERNANCE, RISQUES, CONFORMITE

ISO 37001 Systèmes de Management anti-corruption

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

La norme ISO 37001 définit les exigences pour l'établissement, la mise en œuvre, la tenue à jour, la revue et l'amélioration d'un système de management anti-corruption. Cette norme est conçue pour tous les types d'organismes de tout secteur et pour tout type de corruption que l'on peut rencontrer. En outre, elle peut également être mise en œuvre de façon autonome ou être intégrée avec d'autres systèmes de management.

Devenir un professionnel certifié ISO 37001 vous permet de vous différencier grâce à une expertise démontrée en matière de lutte contre la corruption tout en différenciant votre entreprise de ses concurrents.

Cette norme a pour but de guider, d'identifier, de détecter et de réagir à d'éventuels risques de corruption. Les exigences de cette norme permettent aux organismes de mettre en œuvre un cadre anti-corruption et de mettre en place des politiques et des processus anti-corruption efficaces

Avantages de la certification ISO 37001

1. Compétence validée en management anti-corruption
2. Crédibilité accrue
3. Amélioration des opportunités professionnelles
4. Attractivité accrue sur le marché du travail

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-37001

Formations et objectifs d'apprentissage	Durée
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**

➔➔ S'inscrire

GOUVERNANCE, RISQUES, CONFORMITE

ISO 37301 Systèmes de Management de la Conformité

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

ISO 37301 est une norme de système de management de Type A qui définit les exigences et fournit des lignes directrices pour la création, le développement, la mise en œuvre, l'évaluation, le maintien et l'amélioration continue d'un système de management de la conformité (SMC).

Un SMC fournit aux organisations une approche structurée pour répondre à toutes les obligations de conformité, c'est-à-dire aux exigences auxquelles ils doivent obligatoirement se conformer, telles que les lois, règlements, décisions de justice, permis, licences, ainsi qu'à celles auxquelles ils choisissent volontairement de se conformer, telles que les politiques et procédures internes, codes de conduite, normes et accords avec les communautés ou les ONG.

ISO 37301 est applicable à toutes les organisations, quelles que soient leur taille, leur nature ou la complexité de leur activité. Le SMC est basé sur les principes d'intégrité, de bonne gouvernance, de proportionnalité, de transparence, de responsabilité et de durabilité.

Pour les organisations qui recherchent la croissance et le succès à long terme, l'adhésion constante aux obligations de conformité est une nécessité, pas une option.

Un SMC basé sur les exigences et les lignes directrices d'ISO 37301 dote les organisations d'un ensemble d'outils (politiques, processus et mesures) qui leur permet d'établir et de maintenir une culture de la conformité.

Avantages de la certification ISO 37301

1. Engagement en faveur de la conformité
2. Renforcement des capacités de réduction des risques
3. Culture d'intégrité
4. Encouragement à une conformité proactive

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-37301

GOUVERNANCE, RISQUES, CONFORMITE

Formations et objectifs d'apprentissage	Durée
ISO 37301 Foundation 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**

CMSIA - Auditeur Interne Certifié des Systèmes de Management

Présentation de la norme CMSIA et de son processus de certification

Un audit interne des systèmes de gestion est un processus qui vise à évaluer de manière systématique et indépendante la conformité et l'efficacité d'un système de gestion par rapport à la norme ISO pertinente au sein d'une organisation.

Un audit interne efficace réduit les coûts grâce à une productivité accrue et une meilleure planification, améliore la satisfaction des clients et minimise les barrières entre les services en encourageant la coopération.

La certification d'auditeur interne en systèmes de management atteste qu'une personne possède l'expertise et les connaissances nécessaires pour mettre en place un programme d'audit interne et pour planifier, mener et clôturer des activités d'audit interne.

Avantages de la certification CMSIA

- 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
➔ https://www.chartered-managers.com/pecb/cmsia

Formations et objectifs d'apprentissage	Durée
Certified Management Systems Internal Auditor Développer les compétences nécessaires pour planifier et réaliser des audits internes de systèmes	**3 JOURS**

➔➔ S'inscrire

Pourquoi choisir une carrière en Gouvernance, Risques et Conformité ?

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

Carrières lucratives en Gouvernance, Risques et Conformité ?

Directeur des risques (CRO)
Responsable de la supervision des stratégies de gestion des risques de l'organisation, de l'identification des risques potentiels et du respect des lois et réglementations. Salaire annuel moyen : **219 192 $ US**

Directeur de la gestion des risques
Dirige les politiques et les programmes de gestion des risques et des programmes de gestion des risques, identifie et analyse les risques susceptibles d'avoir un impact sur l'organisation. Salaire annuel moyen : **144 448 $ US**

Responsable du programme GRC
Gère l'ensemble du programme de gouvernance, de gestion des risques et de conformité, en assurant la coordination entre les différents services afin de garantir l'alignement sur les objectifs stratégiques. Salaire annuel moyen : **126 905 $ US**

Responsable de la gouvernance, des risques et de la conformité informatiques
Spécialisé dans la gestion des questions de GRC liées aux technologies de l'information, y compris les risques liés à la cybersécurité et les cadres de gouvernance informatique. Salaire annuel moyen : **132 256 $ US**

Responsable de la conformité
Supervise la fonction de conformité, en veillant à ce que l'organisation respecte les normes légales et aux politiques internes. Salaire annuel moyen : **110 464 $ US**

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

QUALITÉ, SANTÉ, SÉCURITÉ ET DURABILITÉ

Pourquoi la qualité et la gestion ?

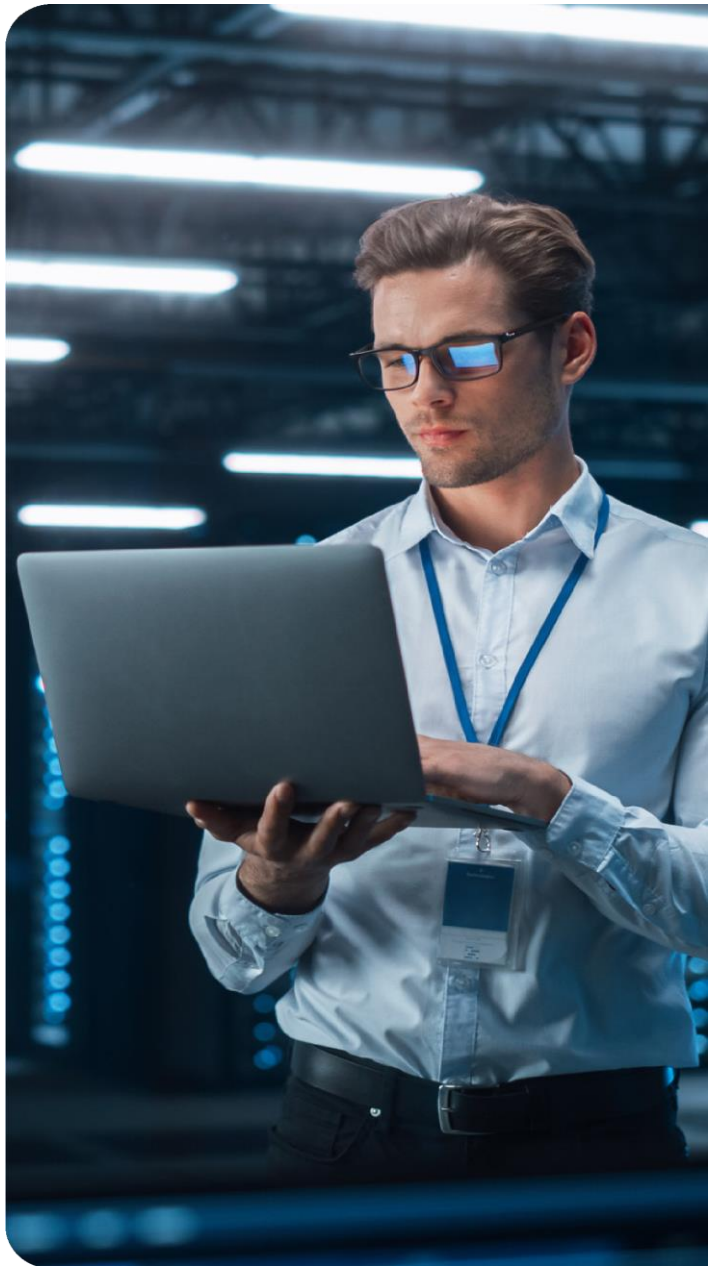
La qualité et la gestion sont essentielles pour permettre aux organisations de maintenir leur cohérence, de satisfaire leurs clients et d'améliorer leurs opérations. Une gestion efficace garantit une utilisation efficiente des ressources et la réalisation des objectifs, tandis que l'accent mis sur la qualité garantit des normes élevées. La combinaison de ces deux éléments contribue à améliorer les processus, à stimuler l'innovation et à favoriser l'amélioration continue, ce qui se traduit par un avantage concurrentiel, une meilleure réputation et un succès durable en phase avec les objectifs commerciaux et les besoins des clients.

Pourquoi la santé et la sécurité ?

La santé et la sécurité sont importantes pour protéger les employés, réduire les risques et garantir la conformité légale. Une culture de sécurité forte prévient les accidents, augmente la productivité et le moral des employés. En donnant la priorité à la santé et à la sécurité, les organisations minimisent les risques juridiques et financiers tout en améliorant leur réputation en matière de pratiques responsables et éthiques. Continuité, résilience et reprise

Pourquoi la durabilité ?

La durabilité est fondamentale pour la santé environnementale, sociale et économique à long terme. Elle contribue à réduire la consommation de 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 - Systèmes de Management de la Qualité

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

1. Démontre une expertise en management de la qualité
2. Évolution de carrière dans des fonctions de management et de direction
3. Évolution de carrière dans des fonctions de management et de direction
4. Carrière Flexible

En savoir plus ➔ https://www.chartered-managers.com/pecb/iso-9001

Formations et objectifs d'apprentissage	Durée
ISO 9001 Foundation ISO 9001 Foundation Comprendre les concepts fondamentaux de la Qualité et les exigences de la norme ISO 9001 relatives à un système de management de la Qualité (SMQ)	**2 JOURS**
ISO 9001 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 Qualité basé sur la norme ISO 9001	**5 JOURS**
ISO 9001 Lead Auditor Acquérir les compétences et les connaissances nécessaires pour réaliser des audits de systèmes de management de la Qualité basés sur la norme ISO 9001 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**

portent

Chartered Managers
EXPERTS ASSOCIES

PECB BEYOND RECOGNITION

Merci de Nous Choisir !

www.pecb.chartered-managers.com