OG SBC

OG Security Business Consulting

www.ogsbc.ma

CATALOGUE

2025-2026

SOMMAIRE

OG Security Business Consulting

HISTORIQUE

OGSBC est née de la vision passionnée de Jamal SAAD, un expert en cybersécurité, qui a choisi le Maroc pour lancer son entreprise. À une époque où les services de consultation en cybersécurité étaient rares dans le pays, Jamal a vu une opportunité unique de faire une différence. En tant que filiale africaine de FOSIR France, OGSBC allie une expertise mondiale à une profonde compréhension des besoins locaux. Nous nous sommes établis comme un pilier de la cybersécurité en Afrique, Offrant des prestations sur mesures aux entreprises de toutes tailles. Notre mission va au-delà du consulting. Nous nous engageons à former et à soutenir la nouvelle génération de professionnels en cybersécurité. En rendant nos services accessibles et en garantissant un excellent rapport qualité-prix, nous contribuons à bâtir un avenir numérique sûr et résilient pour tous.

NOTRE MISSION

Chez OGSBC, nous nous engageons à être le partenaire stratégique de nos clients en matière de cybersécurité. En tant que experts, nous sommes spécialisés dans la gestion de risques, le management de la sécurité du système d'information, les audits approfondis et les certifications PECB et EC-Council. Notre mission est d'apporter une expertise de pointe, une formation de qualité et des webinaires instructifs pour renforcer la résilience numérique de notre communauté . Nous sommes déterminés à assurer la protection des données, à garantir la conformité et à former les professionnels de manière qu'ils prospèrent dans un environnement numérique sécuriséssite durable dans le monde numérique en constante évolution.

NOS VALEURS

Accessibilité

Nous offrons des solutions de pointe à des tarifs accessibles pour garantir une sécurité optimale à tous nos clients.

Transparence

Nous croyons en une communication claire et honnête avec nos clients, garantissant une collaboration basée sur la confiance et la transparence.

Engagement

Nous investissons dans la formation et le soutien des jeunes talents en cybersécurité, contribuant ainsi au développement d'une communauté forte et compétente.

VISION

Nous visons à être le partenaire privilégié de nos clients, contribuant à la sécurité, à la conformité et à la réussite durable dans le monde numérique en constante évolution.

Obtenez votre **certification internationale** avec **OGSBC**

Chez OGSBC, nous ouvrons les portes des certifications internationales les plus reconnues à travers le monde. Grâce à nos partenariats stratégiques avec des organismes de renommée tels que PECB et EC-Council, nous vous offrons un accès privilégié à des programmes de certification en cybersécurité, management de la qualité, continuité des activités, audit, gestion des risques, conformité, et bien plus encore.

En choisissant OGSBC, vous investissez dans une formation rigoureuse, actualisée et orientée terrain, vous permettant non seulement de réussir vos examens de certification, mais aussi d'être immédiatement opérationnel dans vos fonctions. Notre approche est centrée sur l'excellence, la préparation intensive et l'accompagnement personnalisé pour maximiser vos chances de succès.

L'**expertise** technique et pédagogique d'**OGSBC**

Avec plus de 20 ans d'expérience cumulée, OGSBC est un cabinet de formation et de conseil de référence en Afrique et à l'international. Nos formateurs sont des praticiens certifiés, experts dans leur domaine, et dotés d'une pédagogie active et accessible.

Nous croyons à une formation qui allie rigueur académique, expérience terrain et innovation pédagogique. C'est pourquoi nos programmes intègrent des cas pratiques, des mises en situation, et des outils concrets. Notre méthodologie repose sur l'apprentissage par l'action, le feedback permanent et l'adaptation à vos objectifs professionnels.

Nous intervenons aussi bien auprès des entreprises privées que des institutions publiques, avec une capacité à concevoir des formations sur mesure, adaptées aux besoins spécifiques de chaque organisation.

NOS SERVICES

Au-delà de la formation, OGSBC propose une offre complète de services pour accompagner la montée en compétence des professionnels et la transformation des organisations :

01 **Formations certifiantes & sur-mesure**

02 **Audit et conseil en systèmes de management**

03 **Accompagnement à la certification ISO**

04 **Coaching professionnel et organisationnel**

05 **Préparation aux examens internationaux**

06 **Déploiement de projets de transformation digitale**

Nous intervenons dans plusieurs secteurs : santé, éducation, industrie, sécurité, IT, banque, administration publique...
toujours avec un haut niveau d'exigence et d'engagement.

MODES DE FORMATION

Classe virtuelle

Les formations en classe virtuelle d'OGSBC vous offrent la qualité d'une formation en présentiel, dans le confort de votre espace de travail ou de votre domicile. Grâce à des plateforme interactive (zoom, etc..), vous suivez des sessions en direct, animées par des formateurs experts, avec des échanges en temps réel, des ateliers collaboratifs et des supports téléchargeables.
Nos classes virtuelles sont idéales pour ceux qui recherchent flexibilité et interactivité, sans compromis sur la qualité. Chaque session est enregistrée, vous permettant un accès en replay pour revoir les contenus à votre rythme. Le tout dans un environnement structuré, convivial, et propice à l'apprentissage.

E-learning

Le mode E-learning d'OGSBC (ou formation en ligne) est un dispositif d'apprentissage flexible et accessible à distance. Il permet aux apprenants de suivre une formation à leur propre rythme, où qu'ils soient, et selon leur disponibilité. Grâce à une combinaison de vidéos, de documents interactifs, de quiz et parfois de classes virtuelles, ce mode favorise l'autonomie tout en offrant un suivi pédagogique personnalisé.
Le E-learning est idéal pour les professionnels souhaitant concilier montée en compétences et emploi du temps chargé. Il constitue également un excellent choix pour les entreprises cherchant à former efficacement leurs collaborateurs à grande échelle.

MODES DE FORMATION

Self-study

Le mode Self-Study, ou autoformation, permet d'apprendre à son propre rythme, sans formateur ni horaires fixes. Vous recevez tous les supports nécessaires (cours, vidéos, exercices) et vous étudiez quand vous le souhaitez. C'est une solution idéale pour les personnes autonomes qui veulent se former en toute liberté. L'examen peut aussi se passer à distance, à la date de votre choix.

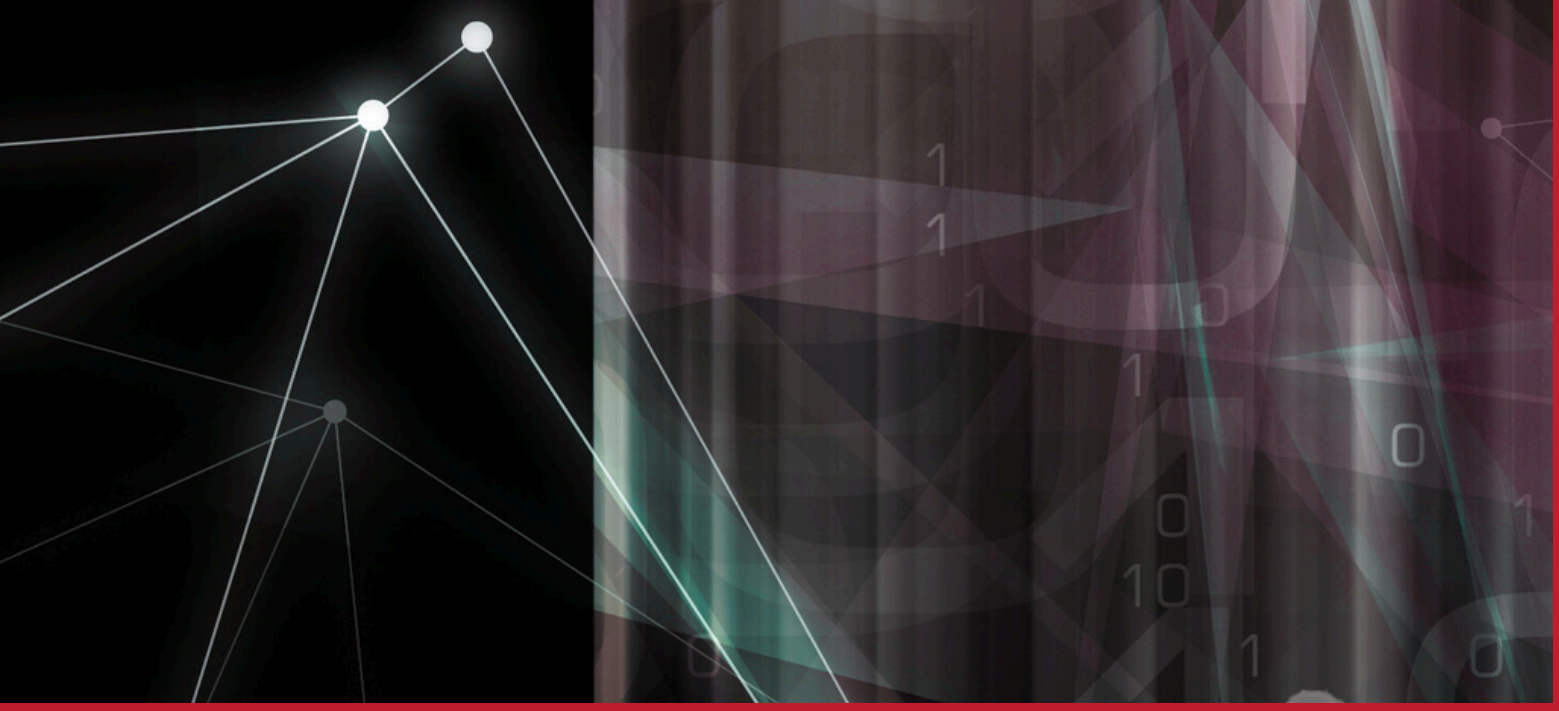
Présentiel

Le mode Présentiel signifie que vous suivez la formation en salle, avec un formateur et d'autres participants. C'est un format classique qui permet d'apprendre avec l'aide directe du formateur, de poser des questions en temps réel, et de participer à des exercices en groupe. L'examen peut être organisé à la fin de la session ou à une date ultérieure.

PECB (Professional Evaluation and Certification Board) est un organisme international de certification reconnu pour son expertise dans la formation et la certification des systèmes de management basés sur les normes ISO. Présent dans plus de 150 pays, PECB propose un large éventail de formations couvrant des domaines clés tels que la qualité (ISO 9001), la sécurité de l'information (ISO/IEC 27001), la continuité des activités (ISO 22301), la gestion environnementale (ISO 14001), la gestion des risques (ISO 31000), et bien d'autres.

Les certifications PECB sont conçues pour accompagner les professionnels dans la mise en œuvre, l'audit et l'amélioration des systèmes de management au sein des organisations. Grâce à des programmes structurés, allant du niveau Foundation au niveau Lead Auditor ou Lead Implementer, les formations PECB combinent une approche théorique rigoureuse avec des études de cas pratiques.

Accrédité selon la norme ISO/IEC 17024, PECB garantit un haut niveau de qualité et de reconnaissance internationale pour ses certifications professionnelles. Ces dernières sont particulièrement recherchées par les experts en conformité, responsables qualité, auditeurs internes, consultants et chefs de projet dans tous les secteurs d'activité.



CYBER SECURITY

ISO/IEC 27001 Information Security Management Systems

L'objectif d'un système de gestion de la sécurité de l'information (SMSI) est de mettre en œuvre des mesures permettant d'identifier, de réduire et d'éliminer toutes les menaces dans une organisation, afin de contribuer à la continuité de l'activité.

FR | EN — 5 jours

ISO/IEC 27001 Lead Implementer

Pourquoi devriez-vous y participer?

Cette formation est conçue pour préparer les participants à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur la norme ISO/IEC 27001. Elle vise à fournir une compréhension complète des bonnes pratiques d'un SMSI et un cadre pour sa gestion et son amélioration continues.

Objectifs

- Comprendre la corrélation entre la norme ISO 27001 et la norme ISO 27002
- Maîtriser les concepts, méthodes et techniques pour mettre en œuvre et gérer un SMSI
- Accompagner une organisation dans la mise en œuvre, la gestion et la tenue à jour d'un SMSI
- Conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives à un SMSI

Public

- Responsables de la sécurité ou de la conformité de l'information au sein d'une organisation
- Membres de l'équipe de sécurité de l'information
- Consultants sécurité
- Experts techniques de l'information
- Directeur de Projets
- Responsable Sécurité/RSSI

Prérequis

Une connaissance générale des concepts du SMSI et d'ISO/IEC 27001.

Programme

Jour 1 : Introduction à la norme ISO/IEC 27001 et démarrage de la mise en œuvre d'un SMSI
Jour 2 : Plan de mise en œuvre d'un SMSI
Jour 3 : Mise en œuvre du SMSI
Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification du SMSI
Jour 5 : Examen de certification

5 jours — FR | EN

ISO/IEC 27001 Lead Auditor

Pourquoi devriez-vous y participer?

Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1.

Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO 27001
- Interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur
- Évaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit

Public

- Auditeurs
- Managers ou consultants
- Personnes responsables de maintenir la conformité aux exigences du SMSI
- Experts techniques
- Conseillers experts en management de sécurité de l'information

Prérequis

Une compréhension de base de la norme ISO/IEC 27001 et une connaissance approfondie des principes d'audit.

Programme

Jour 1 : Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001
Jour 2 : Principes d'audit, préparation et initiation d'un audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

FR | EN 2 jours

ISO/IEC 27001 Transition

Pourquoi devriez-vous y participer?

Cette formation fournit des informations détaillées sur les articles révisés, la nouvelle terminologie, et les différences dans les mesures de l'annexe A. De plus, cette formation offre aux participants les connaissances nécessaires pour soutenir les organisations dans la planification et la mise en œuvre des changements dans leur SMSI afin d'assurer la conformité avec la norme ISO/IEC 27001:2022

Objectifs

- Expliquer les différences entre les normes ISO/IEC 27001:2013 et ISO/IEC 27001:2022
- Interpréter les nouveaux concepts et les nouvelles exigences de la norme ISO/IEC 27001:2022
- Planifier et mettre en œuvre les changements nécessaires à un SMSI existant conformément à la norme ISO/IEC 27001:2022

Public

- Personnes souhaitant rester à jour avec les exigences de la norme ISO/IEC 27001 pour un SMSI
- Personnes cherchant à comprendre les différences entre les exigences de la ISO/IEC 27001:2013 et celles de la ISO 27001:2022
- Personnes chargées d'assurer la transition d'un SMSI de la norme ISO/IEC 27001:2013 à la norme ISO/IEC 27001:2022
- Responsables, formateurs et consultants impliqués dans le maintien d'un SMSI
- Professionnels souhaitant mettre à jour leur certification à la norme ISO/IEC 27001

Programme

Jour 1 : Introduction à la norme ISO/IEC 27001:2022 et comparaison avec la norme ISO/IEC 27001:2013
Jour 2 : Comparaison entre les mesures de l'Annexe A de la norme ISO/IEC 27001:2013 et de la norme ISO/IEC 27001:2022

Examen : 1h

Domaine 1 : Différences entre les principaux articles des normes ISO/IEC 27001:2013 et ISO/IEC 27001:2022
Domaine 2 : Différences entre les mesures de l'Annexe A de la norme ISO/IEC 27001:2013 et celles de la norme ISO/IEC 27001:2022

ISO/IEC 27002 Information Security Controls

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

5 jours FR | EN

ISO/IEC 27002 Manager

Pourquoi devriez-vous y participer?

La certification PECB ISO/IEC 27002 Manager vous permettra de démontrer vos connaissances approfondies en matière de mise en œuvre et de gestion des mesures de sécurité de l'information conformément aux bonnes pratiques de l'industrie.

Objectifs

- Expliquer les concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée basés sur ISO/IEC 27002
- Discuter de la corrélation entre les normes ISO/IEC 27001 et ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Soutenir une organisation dans la détermination, la mise en œuvre et la gestion efficaces des mesures de sécurité de l'information basées sur ISO/IEC 27002

Public

- Responsables impliqués dans la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur ISO/IEC 27001
- Professionnels de l'informatique et consultants désireux d'améliorer leurs connaissances en matière de sécurité de l'information
- Membres d'une équipe de mise en œuvre d'un SMSI ou de sécurité de l'information
- Personnes responsables de la sécurité de l'information au sein d'une organisation

Prérequis

une compréhension fondamentale des exigences de la norme ISO/IEC 27002 et une connaissance approfondie de la sécurité de l'information.

Programme

Jour 1 : Introduction à la norme ISO/IEC 27002
Jour 2 : Ressources d'information, mesures relatives aux personnes, mesures physiques et mesures relatives à la sécurité opérationnelle
Jour 3 : Management des incidents de sécurité de l'information et suivi des mesures relatives à la sécurité de l'information et examen de certification

FR | EN — 5 jours

ISO/IEC 27002 Lead Manager

Pourquoi devriez-vous y participer?

La certification PECB ISO/IEC 27002 Lead Manager est la preuve que vous avez acquis l'expertise nécessaire pour définir les mesures de sécurité de l'information adéquates nécessaires pour traiter les risques identifiés par un processus d'évaluation des risques.

Objectifs

- Maîtriser les concepts clés de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée selon la norme ISO/IEC 27002.
- Comprendre les relations entre la norme ISO/IEC 27002, la norme ISO/IEC 27001 et d'autres cadres réglementaires.
- Savoir interpréter, mettre en œuvre et gérer efficacement les mesures de sécurité de l'information dans le contexte d'un organisme.

Public

- Managers, consultants et professionnels de l'informatique souhaitant renforcer leurs compétences en sécurité de l'information.
- Responsables de la sécurité, de la conformité, du risque ou de la gouvernance au sein d'une organisation.
- Membres d'équipes en charge de la mise en œuvre ou de la gestion d'un SMSI selon la norme ISO/IEC 27001.

Prérequis

une connaissance fondamentale de la norme ISO/IEC 27002 et une connaissance approfondie des mesures de sécurité de l'information

Programme

- Jour 1 : Introduction à la norme ISO/IEC 27002
- Jour 2 : Rôles et responsabilités en matière de sécurité de l'information, de mesures relatives aux personnes et de mesures physiques.
- Jour 3 : Actifs de sécurité de l'information, contrôles d'accès et protection des systèmes et réseaux d'information
- Jour 4 : Gestion des incidents de sécurité de l'information et test et surveillance des mesures de sécurité de l'information conformément à la norme ISO/IEC 27002
- Jour 5 : Examen de certification

PECB Chief Information Security Officer (CISO)

La formation Chief Information Security Officer (CISO) vise à doter les RSSI des compétences et stratégies essentielles pour piloter un programme de sécurité efficace. Elle prépare à protéger les informations et actifs dans un environnement numérique en constante évolution.

5 jours — Anglais

CISO - Training Course & Certification

Pourquoi devriez-vous y participer?

Cette formation vous fournit des informations précieuses et vous permet de développer une compréhension globale du rôle d'un RSSI et des étapes nécessaires pour gérer efficacement la sécurité de l'information au sein d'un organisme

Objectifs

- Expliquer les principes fondamentaux de la sécurité de l'information et les responsabilités du RSSI.
- Concevoir un programme de sécurité efficace conforme aux cadres, lois et politiques en vigueur.
- Évaluer et traiter les risques liés à la sécurité de l'information de manière structurée.

Public

- Professionnels de la sécurité de l'information, de l'informatique et de la gestion des risques souhaitant évoluer vers des postes de direction.
- RSSI expérimentés et responsables souhaitant renforcer leurs compétences, leur leadership et leur veille stratégique.
- Cadres et décideurs impliqués dans la gouvernance et les décisions liées à la sécurité de l'information.

Prérequis

Une compréhension fondamentale des principes et des concepts de la sécurité de l'information.

Programme

Jour 1 : Fondamentaux de la sécurité de l'information et rôle d'un RSSI

Jour 2 : Programme de conformité en matière de sécurité de l'information, gestion des risques, architecture et conception de la sécurité

Jour 3 : Mesures de sécurité, gestion des incidents et gestion des changements

Jour 4 : Sensibilisation à la sécurité de l'information, surveillance et mesurage, amélioration continue

Jour 5 : Examen de certification

Information Security & Risk Management

C'est un domaine qui vise à protéger les informations contre les menaces en assurant leur confidentialité, leur intégrité et leur disponibilité. Il comprend l'identification, l'évaluation et le traitement des risques afin de garantir la continuité des activités et d'atteindre les objectifs de l'organisation en toute sécurité.

FR | EN — 5 jours

ISO/IEC 27005:2022 Risk Manager

Pourquoi devriez-vous y participer?

La formation ISO/IEC 27005:2022 Risk Manager vous enseigne les principes essentiels de gestion des risques selon ISO/IEC 27005 et ISO 31000. Elle vous prépare à identifier, analyser, évaluer et traiter les risques de sécurité de l'information efficacement. En réussissant l'examen, vous obtenez la certification PECB qui valide vos compétences en gestion des risques.

Objectifs

- Explain the risk management concepts and principles outlined by ISO/IEC 27005:2022 and ISO 31000
- Establish, maintain, and improve an information security risk management framework based on the guidelines of ISO/IEC 27005:2022
- Apply information security risk management processes based on the guidelines of ISO/IEC 27005:2022
- Plan and establish risk communication and consultation activities

Public

- Managers ou consultants responsables de la sécurité de l'information
- Responsables de la gestion des risques en sécurité de l'information
- Membres des équipes de sécurité de l'information
- Professionnels IT et privacy officers
- Personnes en charge de la conformité ISO/IEC 27001
- Chefs de projet, consultants ou experts en gestion des risques

Prérequis

Notions de base en sécurité de l'information et connaissance générale de l'ISO/IEC 27001 recommandées.

Programme

Jour 1 : Introduction à l'ISO/IEC 27005:2022 et à la gestion des risques

Jour 2 : Appréciation des risques, traitement des risques, communication et consultation sur les risques selon l'ISO/IEC 27005:2022

Jour 3 : Enregistrement et rapport des risques, surveillance et revue, et méthodes d'évaluation des risques

5 jours — Anglais

EBIOS Risk Manager - Training Course & Certification

Pourquoi devriez-vous y participer?

La formation EBIOS Risk Manager vous forme à la gestion des risques en sécurité de l'information selon la méthode EBIOS, avec des exercices pratiques. Vous pouvez ensuite passer l'examen pour obtenir la certification PECB.

Objectifs

- Comprendre les concepts et principes de base de la gestion des risques avec la méthode EBIOS.
- Maîtriser les activités de la méthode EBIOS pour suivre la réalisation des études (pilotage, contrôle, recadrage).
- Savoir interpréter et expliquer les résultats et livrables clés d'une étude EBIOS.
- Acquérir les compétences nécessaires pour réaliser une étude EBIOS complète.
- Développer les capacités à gérer les risques de sécurité des systèmes d'information d'une organisation.
- Être capable d'analyser et de communiquer efficacement les résultats d'une étude EBIOS.

Public

- Professionnels de la gestion des risques.
- Découvrir les principes ISO/IEC 27005.
- Responsables de la gestion des risques info.
- Aspirants à une carrière en gestion des risques.

Prérequis

Une connaissance fondamentale de la gestion des risques.

Programme

Jour 1 : Objectifs et structure de la formation, introduction à la méthode EBIOS RM, atelier sur le périmètre et la base de sécurité, atelier sur les origines des risques.

Jour 2 : Atelier sur les scénarios stratégiques, atelier sur les scénarios opérationnels, atelier sur le traitement des risques, clôture de la formation.

jour 3 : Examen de certification.

ISO/IEC 27035 Information Security Incident Management

ISO/IEC 27035 est une norme qui définit les bonnes pratiques pour gérer les incidents de sécurité de l'information. Elle aide les organisations à détecter, répondre et se remettre efficacement des incidents de cybersécurité. Son objectif est de réduire l'impact des incidents et d'améliorer la résilience face aux menaces.

FR | EN | 5 jours

ISO/IEC 27035 Lead Incident Manager

Pourquoi devriez-vous y participer?

Cette formation est conçue pour préparer les participants à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur la norme ISO/IEC 27001. Elle vise à fournir une compréhension complète des bonnes pratiques d'un SMSI et un cadre pour sa gestion et son amélioration continues.

Objectifs

- Expliquer les principes fondamentaux de la gestion des incidents.
- Développer et mettre en œuvre des plans de réponse aux incidents adaptés à l'organisation.
- Sélectionner une équipe de réponse aux incidents efficace.
- Réaliser des évaluations de risques pour identifier menaces et vulnérabilités.
- Appliquer les bonnes pratiques des normes internationales pour améliorer la réponse aux incidents.
- Conduire des analyses post-incidents et tirer les leçons apprises.

Public

- Managers, consultants et professionnels IT souhaitant approfondir leurs compétences en gestion des incidents de sécurité.
- Professionnels responsables de la création et gestion des équipes de réponse aux incidents (IRT).
- Membres et coordinateurs des équipes de réponse aux incidents.
- Toute personne impliquée dans la gestion et la réponse aux incidents de sécurité.

Prérequis

connaissances générales en gestion des incidents, sécurité de l'information et normes ISO/IEC 27000.

Programme

Jour 1 : Introduction aux concepts de gestion des incidents de sécurité de l'information et à la norme ISO/IEC 27035
Jour 2 : Conception et préparation d'un plan de gestion des incidents de sécurité de l'information
Jour 3 : Détection et déclaration des incidents de sécurité de l'information
Jour 4 : Surveillance et amélioration continue du processus de gestion des incidents de sécurité de l'information
Jour 5 : Examen de certification

Cloud Security

La sécurité cloud protège les données, applications et environnements dans le cloud. Elle garantit confidentialité, intégrité et disponibilité de l'information. Elle assure aussi la continuité des activités grâce à des contrôles de sécurité adaptés.

FR | EN — 5 jours

Lead Cloud Security Manager

Pourquoi devriez-vous y participer?

Cette formation enseigne la planification et la gestion de la sécurité cloud selon les normes ISO/IEC 27017 et 27018. Elle couvre les concepts de sécurité cloud, la gestion des risques et la réponse aux incidents. Après réussite à l'examen, les participants obtiennent une certification reconnue attestant de leurs compétences.

Objectifs

- Maîtriser les concepts, approches et techniques pour gérer efficacement un programme de sécurité cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes.
- Savoir interpréter et appliquer les directives ISO dans le contexte organisationnel.
- Développer les compétences nécessaires pour planifier, mettre en œuvre et gérer un programme de sécurité cloud.

Public

- Professionnels de la sécurité cloud et de la sécurité de l'information souhaitant gérer un programme de sécurité cloud.
- Managers ou consultants voulant maîtriser les meilleures pratiques en sécurité cloud.
- Responsables chargés de la gestion et de la maintenance d'un programme de sécurité cloud.
- Experts techniques cherchant à approfondir leurs connaissances en sécurité cloud.

Prérequis

connaissances de base sur ISO/IEC 27017, ISO/IEC 27018 et les concepts du cloud computing.

Programme

Jour 1 : Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et lancement d'un programme de sécurité cloud
Jour 2 : Gestion des risques de sécurité du cloud computing et contrôles spécifiques au cloud
Jour 3 : Gestion de l'information documentée et sensibilisation à la sécurité cloud, formation
Jour 4 : Gestion des incidents de sécurité cloud, tests, surveillance et amélioration continue
Jour 5 : Examen de certification

Penetration Testing

Le test de pénétration évalue la sécurité des systèmes en identifiant leurs vulnérabilités. Il permet de renforcer la protection contre les cyberattaques et de réduire les risques financiers.

5 jours — FR | EN

Lead Pentest Professional

Pourquoi devriez-vous y participer?

Cette formation prépare à diriger des tests d'intrusion en combinant techniques avancées et compétences managériales, avec un focus sur la pratique et les enjeux métier.

Objectifs

- Comprendre et appliquer les concepts et principes fondamentaux des tests d'intrusion.
- Acquérir des compétences pratiques et utiliser des outils efficaces pour réaliser des tests d'intrusion réussis.
- Planifier et gérer les ressources et le temps nécessaires pour effectuer des tests d'intrusion adaptés aux risques.
- Develop practical skills and knowledge of the key tools and techniques for effective penetration testing.

Public

- IT professionals aiming to enhance their technical skills.
- Auditors wanting to understand penetration testing processes.
- IT and Risk managers seeking deeper knowledge of penetration test benefits.
- Incident handlers and Business Continuity experts using testing in their processes.
- Penetration testers and ethical hackers involved in cybersecurity.

Prérequis

Connaissances de base en tests de pénétration et cybersécurité.

Programme

Jour 1 : Introduction aux tests de pénétration, éthique, planification et définition du périmètre
Jour 2 : Bases techniques, connaissances et techniques (avec exercices pratiques dans tous les domaines)
Jour 3 : Réalisation d'un test de pénétration (utilisation des outils et techniques) et revue des zones testées
Jour 4 : Analyse des résultats, rédaction de rapports et suivi
Jour 5 : Examen de certification

ISO/IEC 27033 Network Security

La série de normes ISO/IEC 27033 comprend six parties visant à assurer la sécurité réseau des dispositifs, applications, services et utilisateurs finaux. Elle traite de la sécurisation des communications entre réseaux via des passerelles de sécurité, des réseaux privés virtuels (VPN) et l'accès aux réseaux IP sans fil.

FR | EN — 5 jours

ISO/IEC 27033 Lead Network Security Manager

Pourquoi devriez-vous y participer?

La sécurité réseau protège l'infrastructure en assurant confidentialité, intégrité et disponibilité.
Cette formation développe les compétences pour gérer efficacement la sécurité réseau.
Elle couvre les normes ISO/IEC 27033 : conception, concepts clés et communications sécurisées.

Objectifs

- Comprendre les concepts et méthodes clés de la gestion efficace de la sécurité réseau.
- Identifier les liens entre les normes ISO/IEC 27033 et d'autres cadres réglementaires.
- Interpréter et appliquer les lignes directrices ISO/IEC 27033 dans un contexte organisationnel.
- Acquérir les compétences pour soutenir et conseiller une organisation sur la planification, la mise en œuvre et le maintien de la sécurité réseau.

Public

- Professionnels de la sécurité réseau et de la sécurité de l'information souhaitant gérer la sécurité réseau
- Managers ou consultants cherchant à maîtriser les bonnes pratiques en sécurité réseau
- Personnes impliquées dans la planification et la mise en œuvre des aspects architecturaux de la sécurité réseau
- Experts techniques souhaitant approfondir leurs connaissances en sécurité réseau
- Conseillers experts en sécurité réseau

Prérequis

LUne compréhension de base de la série de normes ISO/IEC 27033 ainsi qu'une connaissance générale des concepts de sécurité réseau.

Programme

Jour 1 : Introduction à la série de normes ISO/IEC 27033 et démarrage de la mise en œuvre de la sécurité réseau
Jour 2 : Équipe de sécurité réseau, politique, gestion des risques et gestion de la documentation
Jour 3 : Services d'accès à Internet, segmentation réseau, sécurisation des communications via passerelles, VPN et accès sans fil
Jour 4 : Tests de sécurité réseau, gestion des incidents, surveillance et amélioration continue
Jour 5 : Examen de certification

NIS 2 DIRECTIVE

Entrée en vigueur en janvier 2023, la directive NIS 2 renforce la cybersécurité des secteurs critiques en imposant des mesures strictes et un signalement rapide des incidents. Elle élargit son champ d'application et aide les organisations à mieux se protéger contre les cybermenaces.

5 jours — FR | EN

NIS 2 Directive Lead Implementer

Pourquoi devriez-vous y participer?

Face à la montée des cybermenaces, la directive NIS 2 renforce la sécurité des secteurs critiques. Participer à la formation permet de maîtriser ses exigences, de mettre en œuvre des mesures efficaces.

Objectifs

- Comprendre les principes et exigences clés de la directive NIS 2.
- Mettre en œuvre un programme de cybersécurité conforme à la directive.
- Adapter les exigences NIS 2 au contexte de votre organisme.
- Planifier, gérer et améliorer en continu la conformité NIS 2.

Public

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

Prérequis

Avoir une compréhension fondamentale de la cybersécurité.

Programme

Jour 1 : Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2
Jour 2 : Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques
Jour 3 : Contrôles de cybersécurité, gestion des incidents et gestion des crises
Jour 4 : Communication, tests, surveillance et amélioration continue de la cybersécurité
Jour 5 : Examen de certification

Autres formations

Codes	Formation	Durée	Modes
CM011LCSM	Lead Cloud Security Manager	5 jours	self-study
CM02CFF	Computer Forensics Foundation	2 jours	self-study
CM03LFE	Lead Forensics Examiner	5 jours	self-study
CM04CF	Cybersecurity Foundation	2 jours	self-study
CM05LCM	Lead Cybersecurity Manager	5 jours	self-study
CM06LSSM	Lead SCADA Security Manager	5 jours	self-study
CM07PCF	PECB CMMC Foundations	2 jours	self-study
CM08CCP	CMMC Certified Professional	4 jours	self-study

Ethical Hacking

Le piratage éthique vise à détecter et corriger les vulnérabilités des systèmes informatiques avec l'accord de l'organisation. Il utilise les mêmes techniques que les hackers, mais dans un cadre légal et sécurisé.

FR | EN — 5 jours

Lead Ethical Hacker

Pourquoi devriez-vous y participer?

L'augmentation des cyberattaques fait du piratage éthique un outil essentiel pour protéger les organisations et leurs données. La formation combine théorie, pratique en laboratoire, et examen pour vous préparer efficacement à ce rôle clé en sécurité.

Objectifs

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

Public

- Toute personne souhaitant maîtriser les techniques de tests d'intrusion et de piratage éthique
- Professionnels de la cybersécurité et responsables de la sécurité de l'information
- Membres d'équipes sécurité souhaitant renforcer leurs compétences
- Managers, conseillers ou experts techniques impliqués dans la gestion ou la réalisation de tests d'intrusion

Prérequis

Une bonne connaissance de la sécurité de l'information, des systèmes d'exploitation, des réseaux et des bases en programmation.

Programme

Jour 1 : Introduction au piratage éthique
Jour 2 : Lancement de la phase de reconnaissance
Jour 3 : Lancement de la phase d'exploitation
Jour 4 : Post-exploitation et rapports
Jour 5 : Examen de certification

CONTINUITY, RESILIENCE, AND RECOVERY

Digital Operational Resilience Act (DORA)

La résilience opérationnelle numérique est la capacité d'une entité financière à maintenir la sécurité et la continuité de ses services numériques, même en cas d'incident.
Le règlement DORA renforce cette capacité face aux cybermenaces grandissantes.

FR | EN — 5 jours

DORA Lead Manager

Pourquoi devriez-vous y participer?

Avec l'arrivée de DORA en janvier 2025, cette formation vous prépare à en maîtriser les exigences et à renforcer la résilience numérique face aux risques TIC. Elle offre échanges, bonnes pratiques et outils concrets pour agir efficacement.

Objectifs

- Comprendre les exigences du règlement DORA et ses cinq piliers clés
- Mettre en œuvre des stratégies pour renforcer la résilience et réduire les risques TIC
- Gérer les risques liés aux TIC et assurer la continuité d'activité
- Collaborer efficacement avec les parties prenantes pour garantir la conformité durable
- Utiliser des outils adaptés pour suivre et maîtriser les risques et vulnérabilités TIC

Public

- Cadres supérieurs et décideurs des institutions financières
- Responsables de la conformité et gestionnaires de risques
- Professionnels des TI
- Personnel des affaires juridiques et réglementaires
- Consultants et conseillers spécialisés dans la règlementation financière et la cybersécurité

Prérequis

Une compréhension de base de la sécurité de l'information, de la cybersécurité et des principes de gestion des risques TIC.

Programme

Jour 1 : Introduction des concepts et exigences de DORA
Jour 2 : Gestion des risques et incidents liés aux TIC
Jour 3 : Gestion des risques lies aux prestataires tiers et partage des informations
Jour 4 : Réévaluation et amélioration continuelle
Jour 5 : Examen de certification

ISO 22301 Business Continuity Management System

ISO 22301 définit les exigences pour garantir la continuité des activités et la résilience face aux disruptions.
Cette norme aide les professionnels à gérer efficacement les crises et à assurer la stabilité opérationnelle.

5 jours — FR | EN

ISO 22301 Lead Implementer

Pourquoi devriez-vous y participer?

Les catastrophes peuvent frapper à tout moment ; ISO 22301 vous aide à assurer la continuité des activités face aux crises.
Cette formation vous permet de maîtriser la mise en œuvre d'un système de management de la continuité d'activité efficace.

Objectifs

- Expliquer les principes clés d'un SMCA selon la norme ISO 22301
- Comprendre les exigences ISO 22301 du point de vue d'un responsable de mise en œuvre
- Lancer et planifier la mise en œuvre d'un SMCA conforme à ISO 22301
- Appliquer les bonnes pratiques pour améliorer l'efficacité d'un SMCA
- Interpréter les exigences d'un audit de certification ISO 22301

Public

- Les managers et les consultants impliqués dans la continuité d'activité
- Les personnes désireuses de maîtriser la mise en œuvre d'un système de management de la continuité d'activité
- Les personnes chargées d'assurer et de maintenir la conformité aux exigences du SMCA au sein d'un organisme
- Les personnes qui ont des rôles ou responsabilités liés au SMCA

Prérequis

Une compréhension fondamentale des concepts et principes de la continuité d'activité.

Programme

Jour 1 : Introduction à la norme ISO 22301 et lancement de la mise en œuvre d'un SMCA
Jour 2 : Plan de mise en œuvre d'un SMCA
Jour 3 : Mise en œuvre d'un SMCA
Jour 4 : Évaluation de la performance, amélioration continue et préparation à l'audit de certification
Jour 5 : Examen de certification

FR | EN 5 jours

ISO 22301 Lead Auditor

Pourquoi devriez-vous y participer?

Cette formation ISO 22301 Lead Auditor vous forme à auditer les SMCA selon les normes internationales. Elle vous prépare à évaluer la conformité et à renforcer la résilience des organismes face aux disruptions.

Objectifs

- Expliquer les principes clés d'un SMCA selon ISO 22301
- Interpréter les exigences ISO 22301 en tant qu'auditeur
- Évaluer la conformité d'un SMCA selon les principes d'audit
- Planifier et conduire un audit ISO 22301 selon les normes ISO 19011 et 17021-1
- Gérer un programme d'audit ISO 22301

Public

- Auditeurs chargés de réaliser ou diriger des audits SMCA
- Managers ou consultants maîtrisant l'audit du SMCA
- Responsables de la conformité au SMCA
- Experts techniques se préparant aux audits SMCA
- Conseillers en continuité d'activité

Prérequis

Maîtriser les concepts de continuité d'activité et posséder une bonne connaissance des principes d'audit du SMCA.

Programme

Jour 1 : Introduction au système de management de la continuité d'activité (SMCA) et à la norme ISO 22301
Jour 2 : Principes d'audit, préparation et initiation d'un audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

Autres Formations

Codes	Formation	Durée	Modes
CRR01LDRM	Lead Disaster Recovery Manager	5 Jours	self-study
CRR02PECBCLCM	PECB Certified Lead Crisis Manager	5 Jours	self-study

Nos formations sur Udemy

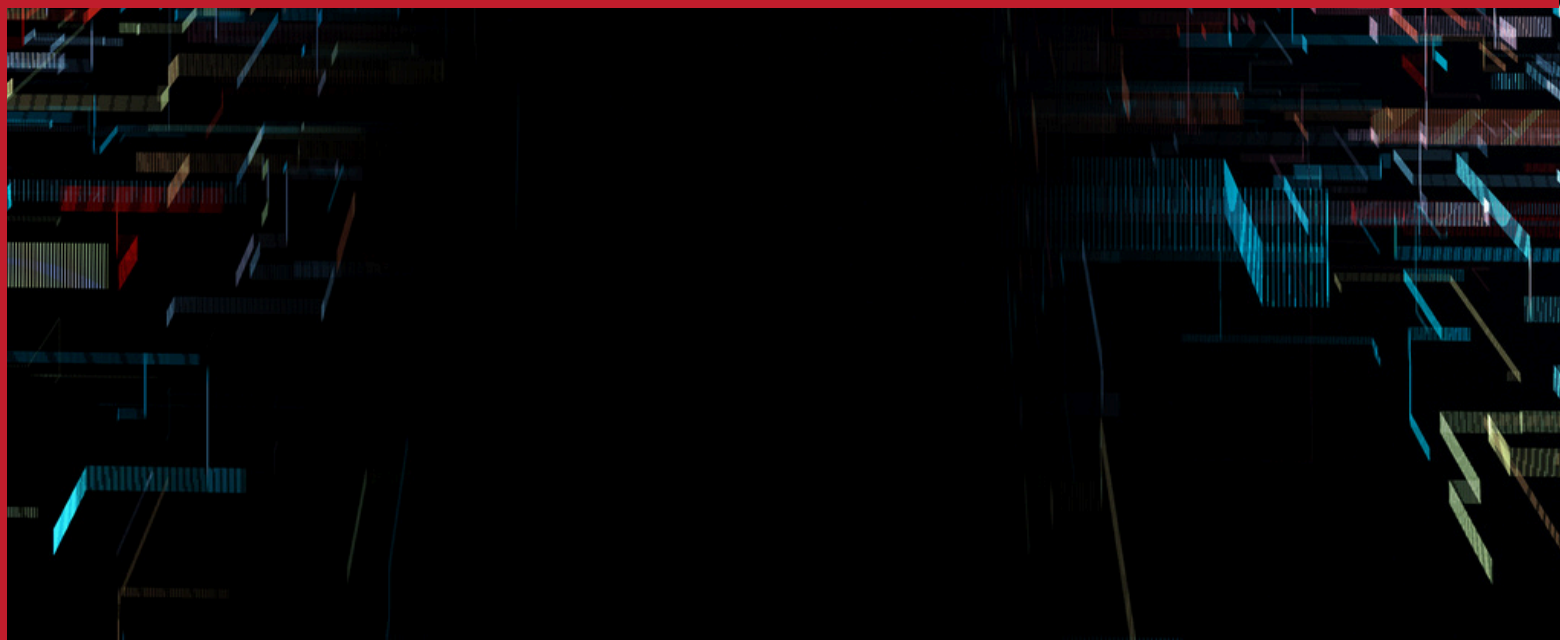
Sensibiliser contre l'ingénierie sociale

Savoir identifier et contrer les cybercriminels en comprenant les pratiques du piratage psychologique.

EBIOS Risk Manager

Comprendre la méthode EBIOS Risk Manager et les principes de base de la gestion des risques.

PRIVACY AND DATA PROTECTION



ISO/IEC 27701 Privacy Information Management System

L'ISO/IEC 27701, publiée en 2019, est la première norme internationale pour la gestion de la protection des données. Elle étend l'ISO 27001 en fournissant un cadre pour implémenter un système de management de la vie privée (PIMS), adaptable à tout organisme quelle que soit sa taille ou localisation.

FR | EN — 5 jours

ISO/IEC 27701 Lead Implementer

Pourquoi devriez-vous y participer?

Ce cours forme les participants à mettre en œuvre un système de management de la vie privée (PIMS) conforme à l'ISO/IEC 27701. Vous y apprendrez les meilleures pratiques pour gérer les données en respectant les régimes de protection de la vie privée.

Objectifs

- Expliquer les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS.
- Comprendre la corrélation entre les normes ISO/IEC 27701, ISO/IEC 27001 ainsi qu'avec d'autres normes et cadres réglementaires.
- Comprendre le fonctionnement d'un PIMS basé sur la norme ISO/IEC 27701 et ses principaux processus.

Public

- Responsables et consultants impliqués dans la gestion de la vie privée et des données
- Conseillers experts cherchant à maîtriser la mise en place d'un système de management de la protection de la vie privée h Personnes responsables des données à caractère personnel (DCP) au sein des organismes
- Personnes chargées de veiller au respect des exigences des régimes de protection de la vie privée

Prérequis

Connaissance de base de l'ISO/IEC 27001 (exigences SMSI)

Programme

Jour 1 : Introduction à l'ISO/IEC 27701 et initiation au PIMS
Jour 2 : Planification de la mise en œuvre d'un PIMS
Jour 3 : Mise en œuvre d'un PIMS
Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification du PIMS
Jour 5 : Examen de certification

5 jours — FR | EN

ISO/IEC 27701 Lead Auditor

Pourquoi devriez-vous y participer?

Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1.

Objectifs

- Comprendre un système de management de la protection de la vie privée (PIMS) et ses processus basés sur ISO/IEC 27701
- Identifier la relation entre ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et les autres normes et cadres réglementaires
- Comprendre le rôle de l'auditeur dans la planification, la direction et le suivi d'un audit de système de management selon ISO 19011
- Apprendre à interpréter les exigences de la norme ISO/IEC 27701 dans le contexte d'un audit du PIMS

Public

- Auditeurs cherchant à réaliser et à diriger des audits de certification du système de management de la protection de la vie privée (PIMS)
- Gestionnaires ou consultants souhaitant maîtriser un processus d'audit du PIMS
- Personnes responsables du maintien de la conformité aux exigences du PIMS
- Experts techniques souhaitant se préparer à un audit du PIMS.
- Experts-conseils en matière de protection des informations d'identification personnelle (IIP)

Prérequis

Maîtrise des concepts clés de la protection des données (RGPD, vie privée, PIMS)

Programme

Jour 1 : Introduction au système de management de la protection de la vie privée (PIMS) et à la norme ISO/IEC 27701
Jour 2 : Principes d'audit, préparation et ouverture d'un audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

GDPR – Certified Data Protection Officer (CDPO)

Acquérez les compétences pour mettre en œuvre et auditer la conformité RGPD, avec une maîtrise des obligations légales, des outils (AIPD, registres) et des bonnes pratiques pour protéger les données personnelles.

FR | EN — 5 jours

GDPR - Certified Data Protection Officer

Pourquoi devriez-vous y participer?

La formation en e-Learning PECB Certified Data Protection Officer vous aidera à acquérir les connaissances et les compétences nécessaires pour servir de délégué à la protection des données (DPO) afin d'aider les organisations à assurer la conformité avec les exigences du Règlement général sur la protection des données (RGPD).

Objectifs

- Comprendre les concepts du RGPD et interpréter ses exigences
- Comprendre le contenu et la corrélation entre le Règlement général sur la protection des données et d'autres cadres réglementaires et normes applicables, telles qu'ISO/IEC 27701 et ISO/IEC 29134
- Acquérir la compétence nécessaire pour remplir le rôle et les tâches quotidiennes du délégué à la protection des données au sein d'un organisme

Public

- Gestionnaires ou consultants souhaitant préparer et soutenir un organisme dans la planification, la mise en œuvre et le maintien d'un programme de conformité basé sur le RGPD
- DPO et personnes responsables du maintien de la conformité aux exigences du RGP
- Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité d'activité

Prérequis

Connaissance de base des principes de la protection des données et du cadre juridique (ex : RGPD, lois locales).

Programme

Jour 1 : Introduction aux concepts et principes du RGPD
Jour 2 : Désignation du DPO et analyse du programme de conformité RGPD
Jour 3 : Opérations du DPO
Jour 4 : Surveillance et amélioration continue de la conformité RGPD
Jour 5 : Examen de certification

AI AND DIGITAL TRANSFORMATION

ISO/IEC 42001 Artificial Intelligence Management System

La norme ISO/IEC 42001 est la première norme internationale dédiée à la mise en place d'un système de management de l'intelligence artificielle (AI Management System – AIMS). Elle aide les organisations à utiliser l'intelligence artificielle de manière responsable, éthique, sécurisée et conforme aux exigences légales et réglementaires.

FR | EN — 5 jours

ISO/IEC 42001 Lead Implementer

Pourquoi devriez-vous y participer?

L'intelligence artificielle (IA) est en train de devenir une force motrice du paysage technologique actuel. Son application s'est étendue à de nombreux secteurs. Son expansion rapide a entraîné des défis et des considérations uniques qui exigent une expertise spécifique pour assurer sa mise en œuvre efficace et sa gestion responsable. La formation PECB ISO/IEC 42001 Lead Implementer vous permet de maîtriser la mise en œuvre pratique et la gestion responsable du système de management de l'IA.

Objectifs

- Expliquer les concepts et principes fondamentaux d'un SMIA conformément à la norme ISO/IEC 42001
- Interpréter les exigences de la norme ISO/IEC 42001 applicables à un SMIA du point de vue d'un Implementer (responsable de la mise en œuvre)
- Lancer et planifier la mise en œuvre d'un SMIA conformément à la norme ISO/IEC 42001 en utilisant la méthodologie IMS2 de PECB et d'autres meilleures pratiques

Public

- Professionnels chargés de superviser et de gérer les projets d'IA
- Consultants des stratégies de mise en œuvre de l'IA
- Conseillers experts et spécialistes désirant maîtriser la mise en œuvre pratique d'un SMIA conformément à la norme ISO/IEC 42001
- Personnes chargées de veiller à ce que les projets d'IA soient conformes aux exigences en la matière au sein d'une organisation

Prérequis

Compréhension des systèmes de management (ex : ISO 27001, ISO 9001).
Notions de base sur l'intelligence artificielle et ses enjeux éthiques/réglementaires.

Programme

Jour 1 : Introduction à l'ISO/IEC 42001 et au lancement de la mise en œuvre d'un SMIA
Jour 2 : Plan de mise en œuvre d'un SMIA
Jour 3 : Mise en œuvre d'un SMIA
Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification du SMIA
Jour 5 : Examen de certification

5 jours — FR | EN

ISO/IEC 42001 Lead Auditor

Pourquoi devriez-vous y participer?

La formation ISO/IEC 42001 Lead Auditor est bénéfique pour les professionnels qui souhaitent garder une longueur d'avance sur la concurrence. Cette formation vous permet d'acquérir l'expertise nécessaire pour naviguer dans le domaine complexe des cadres organisationnels influencés par l'IA, vous assurant ainsi d'être bien préparé pour contribuer au succès des organisations dans cette ère de la transformation.

Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de l'IA conformément à la norme ISO/IEC 42001
- Interpréter les exigences de la norme ISO/IEC 42001 relatives à un système de management de l'IA du point de vue d'un auditeur
- Évaluer la conformité d'un système de management de l'IA aux exigences de la norme ISO/IEC 42001, dans le respect des concepts et principes fondamentaux de l'audit

Public

- Personnes ayant une expérience en matière d'audit, interne ou externe, désirant se spécialiser dans l'audit des systèmes de management de l'IA
- Gestionnaires ou consultants souhaitant maîtriser le processus d'audit des systèmes de management de l'IA
- Personnes responsables du maintien de la conformité aux exigences du système de management de l'IA au sein d'une organisation h Conseillers experts en management de l'IA

Prérequis

Maîtrise de l'ISO 42001 (exigences de base pour les systèmes de management de l'IA).

Programme

Jour 1 : Introduction au système de management de l'intelligence artificielle et à la norme ISO/IEC 42001
Jour 2: Principes d'audit, préparation et lancement d'un audit
Jour 3: Activités d'audit sur place
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

Digital Transformation

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.

FR | EN 5 jours

Digital Transformation Officer

Pourquoi devriez-vous y participer?

La formation PECB Certified Digital Transformation Officer fournit des informations pertinentes qui aideront les participants à acquérir une connaissance complète en matière de transformation numérique et des étapes requises pour assurer la transformation numérique d'un modèle d'entreprise. Ce cours aborde également des notions approfondies sur les méthodologies et les approches relatives à la transformation numérique. De plus, elle offre aux participants des connaissances sur certaines des technologies les plus usuelles, tel que l'intelligence artificielle, l'apprentissage automatique, l'IoT, la blockchain, le cloud computing et le big data.

Objectifs

- Expliquer les concepts fondamentaux de la transformation numérique et des technologies de transformation numérique, notamment l'intelligence artificielle, le cloud computing, le big data, l'apprentissage automatique, l'IoT et la blockchain
- Maîtriser les approches et méthodologies utilisées pour la mise en œuvre des stratégies de transformation numérique dans un organisme
- Favoriser l'efficacité d'un organisme dans la conception, la mise en œuvre, la surveillance et l'amélioration d'une stratégie de transformation numérique

Public

- Responsables et dirigeants qui souhaitent se perfectionner dans l'économie numérique
- Professionnels chargés de transformer les opérations d'un organisme par le moyen de technologies numériques
- Spécialistes de l'informatique ou aux consultants qui souhaitent améliorer leurs connaissances en matière de conception et de stratégie numériques afin de soutenir les initiatives de transformation numérique d'un organisme

Prérequis

Maîtrise des enjeux du numérique (IA, cloud, IoT, blockchain).

Programme

Jour 1 : Introduction à la transformation numérique
Jour2: Technologies, approches et méthodologies de la transformation numérique et planification de la stratégie de transformation numérique
Jour 3: Gestion des risques liés à la transformation numérique et mise en œuvre de la stratégie de transformation numérique
Jour 4: Communication et surveillance de la stratégie de transformation numérique
Jour 5: Examen de certification

GOVERNANCE, RISK, AND COMPLIANCE

ISO 31000 Risk Management

L'ISO 31000 fournit un cadre pour identifier, évaluer et maîtriser les risques, en intégrant la gestion des risques à tous les niveaux de l'organisation. Elle s'applique à tous types de risques et d'organismes, et renforce stabilité et résilience.

FR | EN — 3 jours

ISO 31000 Risk Manager

Pourquoi devriez-vous y participer?

La formation ISO 31000 vous apporte les compétences essentielles pour gérer les risques de manière structurée et efficace.
Elle vous prépare à intégrer le management du risque dans les processus organisationnels.

Objectifs

- Démontrer leur compréhension des principes de management du risque, tels que formulés dans ISO 31000
- Établir, maintenir et améliorer continuellement un cadre de management du risque, conformément aux lignes directrices d'ISO 31000
- Appliquer le processus de management du risque, conformément aux lignes directrices d'ISO 31000

Public

- Gestionnaires ou consultants chargés du management efficace du risque dans un organisme
- Toute personne désirant acquérir des connaissances approfondies sur les concepts, processus et principes de management du risque
- Conseillers impliqués dans le management du risque

Prérequis

Des connaissances fondamentales de la norme ISO 31000 et des connaissances approfondies sur le management du risque

Programme

Jour 1 : Introduction aux principes et au cadre organisationnel de l'ISO 31000
Jour 2 : Processus de management du risque conforme à la norme ISO 31000
Jour 3 : Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010 et examen de certification

ISO 37001 Anti-Bribery Management System

La norme ISO 37001 définit les exigences pour prévenir, détecter et traiter les risques de corruption dans tout type d'organisme. Elle aide à renforcer l'intégrité, à se conformer aux lois anti-corruption et à instaurer une culture éthique.
Se former et se certifier ISO 37001 valorise votre expertise et crédibilise l'engagement anti-corruption de votre organisation.

5 jours — FR | EN

ISO 37001 Lead Implementer

Pourquoi devriez-vous y participer?

La formation ISO 37001 Lead Implementer vous prépare à concevoir, déployer et gérer un système de management anti-corruption efficace. Elle vous dote des compétences nécessaires pour prévenir et traiter les risques de corruption dans tout organisme.

Objectifs

- Comprendre les principes clés d'un SMAC selon ISO 37001
- Interpréter les exigences de la norme en tant que responsable de mise en œuvre
- Planifier et initier un SMAC avec la méthode IMS2 et les bonnes pratiques
- Accompagner l'organisme dans la gestion et l'amélioration continue du SMAC
- Préparer à un audit de certification par un tiers indépendant

Public

- Responsables ou consultants impliqués dans le management anti-corruption
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management anti-corruption
- Toute personne responsable du maintien de la conformité aux exigences du SMAC
- Membres d'une équipe du SMAC

Prérequis

Une bonne connaissance de la norme ISO 37001 et des connaissances approfondies des principes de sa mise en œuvre.

Programme

Jour 1 : Introduction à la norme ISO 37001 et initialisation d'un SMAC
Jour 2 : Planification de la mise en œuvre d'un SMAC
Jour 3 : Mise en œuvre d'un SMAC
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMAC
Jour 5 : Examen de certification

ISO 37301 Compliance Management System

ISO 37301 définit les exigences pour mettre en place un système de management de la conformité (SMC) couvrant les obligations légales et volontaires. Applicable à toute organisation, il repose sur les principes d'intégrité, de transparence et de gouvernance. Grâce à sa structure HLS, il peut être intégré à d'autres systèmes de management.

FR | EN — 5 jours

ISO 37301 Lead Implementer

Pourquoi devriez-vous y participer?

La norme ISO 37301 aide à éviter les risques de non-conformité et à promouvoir l'éthique, la transparence et la durabilité.
La formation Lead Implementer vous permet d'acquérir les compétences nécessaires pour mettre en œuvre et maintenir un système de management de la conformité. Elle mène à une certification reconnue, validant votre expertise professionnelle.

Objectifs

- Présenter concepts, méthodes et techniques pour une mise en œuvre efficace d'un SMC.
- Expliquer les liens entre ISO 37301 et autres normes ou cadres réglementaires.
- Interpréter les exigences ISO 37301 du point de vue du responsable de mise en œuvre.
- Accompagner les organisations dans la création, le maintien et l'amélioration continue du SMC.
- Préparer les organisations aux audits de certification par des tiers.

Public

- Managers, consultants et responsables conformité cherchant à maîtriser ISO 37301
- Responsables en charge de la diligence raisonnable et du management des risques de conformité
- Acteurs de la gouvernance, du management des risques et de la conformité
- Professionnels souhaitant promouvoir l'intégrité et l'éthique en organisation
- Futurs agents de conformité ou consultants spécialisés en management de la conformité

Prérequis

Une connaissance de base des normes ISO relatives aux systèmes de management, ainsi qu'une compréhension générale de la norme ISO 37301 (ou ISO 19600) et des principes de mise en œuvre du SM.

Programme

Jour 1 : Introduction à ISO 37301 et initiation de la mise en œuvre d'un SMC
Jour 2 : Mise en œuvre d'un SMC
Jour 3 : Mise en œuvre d'un SMC
Jour 4 : Surveillance, amélioration continue et préparation à l'audit de certification du SMC
Jour 5 : Examen de certification

5 jours — FR | EN

ISO 37301 Lead Auditor

Pourquoi devriez-vous y participer?

La formation PECB 37301 Lead Auditor vous forme à auditer un système de management de la conformité selon ISO 37301, en suivant les normes ISO 19011 et ISO/IEC 17021-1. Elle inclut des exercices pratiques pour maîtriser les techniques d'audit et la rédaction de rapports.

Objectifs

- Comprendre les concepts clés et processus d'un SMC selon ISO 37301.
- Connaître les liens entre ISO 37301 et autres normes/cadres réglementaires.
- Saisir le rôle de l'auditeur pour planifier, conduire et suivre un audit selon ISO 19011.
- Interpréter les exigences ISO 37301 dans le cadre d'un audit SMC.
- Planifier l'audit, diriger l'équipe, rédiger les rapports et assurer le suivi.
- Appliquer la diligence professionnelle tout au long de l'audit.

Public

- Auditeurs souhaitant effectuer et diriger des audits SMC
- Responsables ou consultants cherchant à maîtriser le processus d'audit du SMC
- Personnes responsables du maintien de la conformité aux exigences de la norme ISO 37301 dans une organisation
- Experts techniques cherchant à se préparer à un audit du SMC
- Conseillers spécialisés et responsables de la conformité

Prérequis

Une compréhension fondamentale des exigences de la norme ISO 37301 (ou des lignes directrices de la norme ISO 19600) pour un SMC et une connaissance approfondie des principes d'audit.

Programme

Jour 1 : Introduction au système de management de la conformité (SMC) et à la norme ISO 37301
Jour 2 : Principes d'audit et préparation pour le lancement d'un audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

Autres Formations

Codes	Formation	Durée	Modes
GRC01F	ISO/IEC 38500 Foundation	2 Jours	self-study
GRC02ITCGM	ISO/IEC 38500 IT Corporate Governance Manager	3 Jours	self-study
GRC03LITCGM	ISO/IEC 38500 Lead IT Corporate Governance Manager	5 Jours	self-study
GRC02MSIA	Management Systems Internal Auditor	3 Jours	self-study
GRC03CMSC	Certified Management Systems Consultant (CMSC)	3 Jours	self-study

QUALITY, HEALTH, SAFETY AND SUSTAINABILITY

ISO 9001 Quality Management System

La norme ISO 9001 guide les organismes dans la mise en œuvre d'un système de management de la qualité, favorisant l'amélioration continue, la performance globale et une gestion maîtrisée des risques. Elle constitue un levier stratégique pour le développement durable.

FR | EN — 5 jours

ISO 9001 Lead Implementer

Pourquoi devriez-vous y participer?

Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la qualité et à développer vos aptitudes à accroître la satisfaction des clients de l'organisme, améliorer son efficacité et sa performance globale.

Objectifs

- Comprendre les principes de la norme ISO 9001 et sa relation avec d'autres cadres réglementaires.
- Maîtriser les méthodes pour mettre en œuvre, gérer et améliorer un Système de Management de la Qualité (SMQ).
- Acquérir l'expertise pour interpréter les exigences de la norme et conseiller efficacement un organisme.

Public

- Responsables ou consultants impliqués dans le management de la qualité
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la qualité
- Toute personne responsable du maintien de la conformité aux exigences du SMQ
- Membres d'une équipe du SMQ

Prérequis

Une bonne connaissance de la norme ISO 9001 et des connaissances approfondies des principes de mise en œuvre.

Programme

Jour 1 : Introduction à la norme ISO 9001 et initialisation d'un SMQ
Jour 2 : Planification de la mise en œuvre d'un SMQ
Jour 3 : Mise en oeuvre d'un SMQ
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMQ
Jour 5 : Examen de certification

5 jours — FR | EN

ISO 9001 Lead Auditor

Pourquoi devriez-vous y participer?

Outre une base théorique, la formation fournit également des exemples, des exercices et des questionnaires pour vous aider à mettre en pratique les aspects les plus importants des audits d'évaluation de la conformité .

Objectifs

- Comprendre les concepts fondamentaux d'un SMQ selon la norme ISO 9001 et en interpréter les exigences en tant qu'auditeur.
- Évaluer la conformité d'un SMQ à la norme ISO 9001 en s'appuyant sur les principes et bonnes pratiques d'audit.
- Planifier, conduire, clôturer et gérer un programme d'audit ISO 9001 selon les normes ISO/IEC 17021-1 et ISO 19011.

Public

- Auditeurs souhaitant réaliser et diriger des audits de SMQ.
- Professionnels souhaitant adopter la méthodologie AMS2 pour réaliser des audits
- Personnes responsables du maintien de la conformité aux exigences de la norme ISO 9001
- Experts techniques souhaitant se préparer à un audit du SMQ
- Professionnels souhaitant faire carrière dans le domaine de l'évaluation de la conformité

Prérequis

Une compréhension fondamentale des exigences de la norme ISO 9001 pour un SMQ et une connaissance approfondie des principes d'audit.

Programme

Jour 1 : Introduction au système de management de la qualité (SMQ) et à la norme ISO 9001
Jour 2 : Principes d'audit, préparation et lancement d'un audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

ISO/IEC 17025 Laboratory Management System

ISO/IEC 17025 est une norme internationale qui encadre la qualité et la compétence des laboratoires d'essais et d'étalonnages. Elle vise à garantir des résultats fiables et à améliorer la performance des laboratoires. Elle comprend des exigences de gestion et des exigences techniques portant sur le personnel, les équipements et les méthodes.

Français | 5 jours

ISO/IEC 17025 Lead Implementer

Pourquoi devriez-vous y participer?

La formation ISO/IEC 17025 Lead Implementer vous permet d'acquérir les compétences nécessaires pour mettre en place un système de gestion conforme à la norme. Elle vous prépare à garantir des résultats fiables et à obtenir l'accréditation du laboratoire.
En réussissant l'examen, vous obtenez la certification PECB, preuve de votre expertise professionnelle.

Objectifs

- Acquérir une expertise pratique pour mettre en œuvre et gérer efficacement un Système de Management de Laboratoire (LMS) conforme à ISO/IEC 17025.
- Comprendre et interpréter les exigences de la norme dans le contexte réel d'un laboratoire.
- Savoir accompagner un laboratoire dans ses activités de test, de calibration et d'amélioration continue.
- Se préparer à la certification officielle PECB, reconnue à l'international, pour valoriser ses compétences professionnelles.

Public

- Professionnels des laboratoires d'essais et d'étalonnages
- Managers et consultants souhaitant maîtriser la gestion des laboratoires
- Techniciens responsables de la conformité aux exigences d'accréditation
- Personnes soutenant les opérations des laboratoires
- Experts techniques préparant l'évaluation de compétence

Prérequis

Une connaissance approfondie de la norme ISO/IEC 17025 et une connaissance approfondie des principes de mise en œuvre.

Programme

Jour 1 : Introduction à ISO/IEC 17025 et initiation au système de gestion de laboratoire (SGL)
Jour 2 : Planification de la mise en œuvre d'un SGL
Jour 3 : Mise en œuvre d'un SGL
Jour 4 : Suivi, mesure, amélioration continue du SGL et préparation à l'accréditation
Jour 5 : Examen de certification

ISO 21502 Project Management

ISO 21502 est une norme internationale qui fournit des lignes directrices pour aider les chefs de projet et les organisations basées sur des projets à mener à bien leurs projets. Mise à jour de la norme ISO 21500:2012, elle décrit des pratiques efficaces en gestion de projet et peut être appliquée à tout type d'organisation et de projet, quelle que soit leur taille ou secteur.

5 jours | Français

ISO 21502 Lead Project Manager

Pourquoi devriez-vous y participer?

La formation ISO 21502 Lead Project Manager vous permet de maîtriser la gestion de projets selon la norme ISO 21502. Elle allie théorie et exercices pratiques pour une application concrète. Après réussite à l'examen, vous obtenez une certification reconnue internationalement.

Objectifs

- Comprendre les concepts fondamentaux et méthodologies clés de la gestion de projet.
- Savoir mettre en œuvre des pratiques intégrées de gestion de projet conformes à la norme ISO 21502.
- Appliquer des pratiques spécifiques de gestion de projet dans les différentes activités du projet.
- Se préparer efficacement à la certification grâce à des exercices pratiques et des quiz ciblés.

Public

- Chefs de projet
- Sponsors de projet
- Conseillers experts
- Membres des équipes projet
- Cadres, managers et directeurs impliqués dans la gouvernance et les audits de projets
- Personnes souhaitant comprendre la gestion de projet ou progresser dans ce domaine

Prérequis

Une compréhension fondamentale des concepts, des méthodologies et des pratiques de gestion de projet.

Programme

Jour 1 : Introduction à ISO 21502 et gestion de projet
Jour 2 : Pratiques intégrées de gestion de projet
Jour 3 : Pratiques de gestion pour un projet
Jour 4 : Pratiques de gestion pour un projet (suite)
Jour 5 : Examen de certification

Autres Formations

Codes	Formation	Durée	Modes
QM01MDQMSF	ISO 13485 Medical Devices Quality Management System Foundation	2 Jours	self-study
QM02MDQMSLI	ISO 13485 Medical Devices Quality Management System Lead Implementer	5 Jours	self-study
QM03MDQMSLA	ISO 13485 Medical Devices Quality Management System Lead Auditor	5 Jours	self-study
QM04ITSMSF	ISO/IEC 20000 IT Service Management System Foundation	2 Jours	self-study
QM05ITSMSLI	ISO/IEC 20000 IT Service Management System Lead Implementer	5 Jours	self-study
QM06SSYB	Six Sigma Yellow Belt	2 Jours	self-study
QM07SSGB	Six Sigma Green Belt	5 Jours	self-study
QM08EOMSF	ISO 21001 Educational Organizations Management System Foundation	2 Jours	self-study
QM09EOMSLI	ISO 21001 Educational Organizations Management System Lead Implementer	5 Jours	self-study
QM09EOMSLA	ISO 21001 Educational Organizations Management System Lead Auditor	5 Jours	self-study
QM010AMSF	ISO 55001 Asset Management System Foundation	2 Jours	self-study
QM011AMSLI	ISO 55001 Asset Management System Lead Implementer	5 Jours	self-study
QM012AMSLA	ISO 55001 Asset Management System Lead Auditor	5 Jours	self-study
QM013AMST	ISO 55001 Asset Management System Transition	2 Jours	self-study
QM014SCSMSF	ISO 28000 Supply Chain Security Management System Foundation	2 Jours	self-study
QM015SCSMSLI	ISO 28000 Supply Chain Security Management System Lead Implementer	5 Jours	self-study
QM016SCSMSLA	ISO 28000 Supply Chain Security Management System Lead Auditor	5 Jours	self-study
QM017SCSMST	ISO 28000 Supply Chain Security Management System Transition	2 Jours	self-study

ISO 45001 Occupational Health and Safety Management System

ISO 45001 est une norme internationale pour la gestion de la santé et de la sécurité au travail. elle aide à prévenir les accidents et à améliorer les performances en santé et sécurité. elle permet aussi l'intégration avec d'autres systèmes de management comme la qualité et l'environnement.

FR | EN — 5 jours

ISO 45001 Lead Implementer

Pourquoi devriez-vous y participer?

La formation ISO 45001 Lead Implementer vous enseigne à mettre en œuvre un système de santé et sécurité au travail.elle couvre les exigences et meilleures pratiques de la norme ISO 45001. la certification valide vos compétences reconnues internationalement.

Objectifs

- Comprendre les concepts et principes fondamentaux du système de management de la santé et sécurité au travail selon ISO 45001.
- Interpréter les exigences de la norme ISO 45001 du point de vue d'un implémenteur.
- Planifier et initier la mise en œuvre d'un système de management OH&S en utilisant la méthodologie PECB IMS2.
- Soutenir l'organisation dans l'exploitation, la maintenance et l'amélioration continue du système OH&S.

Public

- Personnes responsables de la sécurité au travail et de son amélioration
- Agents, consultants et conseillers en santé et sécurité au travail
- Professionnels souhaitant maîtriser la méthodologie IMS2 de PECB pour l'implémentation d'un système OH&S
- Responsables de la conformité du système OH&S aux exigences ISO 45001
- Membres des équipes de santé et sécurité au travail

Prérequis

Connaissances de base des normes ISO, compréhension d'ISO 45001 et des principes de mise en œuvre exigées.

Programme

Jour 1 : Introduction à ISO 45001 et initiation de la mise en œuvre d'un système de management de la santé et sécurité au travail (OH&S MS)
Jour 2 : Planification de la mise en œuvre d'un OH&S MS
Jour 3 : Mise en œuvre d'un OH&S MS
Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification de l'OH&S
Jour 5 : Examen de certification

5 jours — FR | EN

ISO 45001 Lead Auditor

Pourquoi devriez-vous y participer?

La formation ISO 45001 Lead Auditor vous permettra d'acquérir l'expertise nécessaire pour réaliser des audits de Systèmes de management de la santé et de la sécurité au travail (SMSST) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues.

Objectifs

- Comprendre le fonctionnement d'un Système de management de la santé et de la sécurité au travail, conforme à la norme ISO 45001.
- Expliquer la corrélation entre la norme ISO 45001 et les autres normes et cadres réglementaires .
- Savoir diriger un audit et une équipe d'audit.

Public

- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la santé et la sécurité au travail
- Responsable du maintien de la conformité aux exigences du SMSST
- Experts techniques désirant préparer un audit du Système de management de la santé et de la sécurité au travail

Prérequis

Connaissances de base en santé et sécurité au travail (SST)

Programme

Jour 1 : Introduction au Système de management de la santé et de la sécurité au travail et à la norme ISO 45001....
Jour 2 : Principes, préparation et déclenchement de l'audit..
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

Formations disponibles

Codes	Formation	Durée	Modes
HS01FSMSF	ISO 22000 Food Safety Management System Foundation	2 Jours	self-study
HS02FSMSLI	ISO 22000 Food Safety Management System Lead Implementer	5 Jours	self-study
HS03FSMSLA	ISO 22000 Food Safety Management System Lead Auditor	5 Jours	self-study
HS04SOMSF	ISO 18788 Security Operations Management System Foundation	5 Jours	self-study
HS05SOMSLI	ISO 18788 Security Operations Management System Lead Implementer	5 Jours	self-study
HS06SOMSLA	ISO 18788 Security Operations Management System Lead Auditor	5 Jours	self-study

Nos Webinaires

Devenez Data Protection Officer certifié – Aperçu essentiel

Une formation clé pour exceller en conformité RGPD et protection des données.

Devenez Risk Manager Certifié EBIOS RM – Aperçu essentiel

Actualisez vos compétences et boostez votre carrière en sécurité numérique.

Rôle, missions et obligations du DPO

Découvrez les étapes clés pour devenir un expert en sécurité de l'information et l'importance d'obtenir la certification Lead Implementer.

ISO 14001 Environmental Management System

La norme ISO 14001 est un standard international qui définit les exigences pour un Système de Management Environnemental (SME). Elle aide les organisations à améliorer leur performance environnementale, à respecter les réglementations et à réduire leur impact écologique.

FR | EN — 5 jours

ISO 14001 Lead Implementer

Pourquoi devriez-vous y participer?

La formation ISO 14001 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner un organisme lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management environnemental (SME) conforme à la norme ISO 14001.

Objectifs

- Comprendre la corrélation entre la norme ISO 14001 et la norme ISO 14040, ainsi qu'avec d'autres normes et cadres réglementaires.
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SME.
- Savoir interpréter les exigences de la norme ISO 14001 dans un contexte spécifique de l'organisme.

Public

- Responsables ou consultants impliqués dans le management environnemental.
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management environnemental .
- Toute personne responsable du maintien de la conformité aux exigences du SME .
- Membres d'une équipe du SME.

Prérequis

Avoir une connaissance de base des systèmes de management environnemental et des exigences de la norme ISO 14001.

Programme

Jour 1 : Introduction à la norme ISO 14001 et initialisation d'un SME
Jour 2 : Planification de la mise en œuvre d'un SME
Jour 3 : Mise en œuvre d'un SME
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SME
Jour 5 : Examen de certification

5 jours — FR | EN

ISO 14001 Lead Auditor

Pourquoi devriez-vous y participer?

La formation ISO 14001 Lead Auditor vous permettra d'acquérir l'expertise nécessaire pour réaliser des audits de Systèmes de management environnemental (SME) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues.

Objectifs

- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011.
- Savoir diriger un audit et une équipe d'audit .
- Savoir interpréter les exigences d'ISO 14001 dans le contexte d'un audit du SME.
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Public

- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management environnemental.
- Responsable du maintien de la conformité aux exigences du SME .
- Experts techniques désirant préparer un audit du Système de management environnemental
- Conseillers spécialisés en management environnemental.

Prérequis

Avoir une connaissance préalable des principes de la norme ISO 14001 et des concepts de base en audit des systèmes de management.

Programme

Jour 1 : Introduction au Système de management environnemental et à la norme ISO 14001
Jour 2 : Principes, préparation et déclenchement de l'audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

ISO 26000 Social Responsibility Management System

La norme ISO 26000 fournit des lignes directrices pour intégrer la responsabilité sociétale dans les stratégies et les pratiques des organisations. Elle n'est pas certifiable, mais elle aide les entreprises, institutions et autres entités à opérer de manière éthique, transparente et durable.

FR | EN — 5 jours

ISO 26000 Lead Manager

Pourquoi devriez-vous y participer?

Cette formation vous permet d'acquérir les connaissances et compétences nécessaires pour guider les organisations dans la planification, l'établissement, le maintien, la revue et l'amélioration continue de leurs initiatives stratégiques en matière de responsabilité sociétale, conformément aux lignes directrices de la norme ISO 26000 et à d'autres bonnes pratiques du secteur.

Objectifs

- Expliquer les concepts fondamentaux de la sécurité et les principes de la responsabilité sociétale conformément à la norme ISO 26000.
- Comprendre et identifier les questions centrales et les domaines d'action de la responsabilité sociétale au sein d'une organisation.
- Appliquer des pratiques pour intégrer la responsabilité sociétale dans une organisation.

Public

- Managers ou consultants impliqués dans ou concernés par les efforts de responsabilité sociétale .
- Gestionnaires de projets, consultants et conseillers experts souhaitant en savoir plus sur la responsabilité sociétale et le développement durable.
- Personnes chargées de veiller à ce que l'organisation respecte les lois et réglementations pertinentes en matière de responsabilité sociétale.

Prérequis

Avoir une compréhension de base des principes de développement durable et des enjeux de la responsabilité sociétale.

Programme

Jour 1 : Introduction à la norme ISO 26000 et à la responsabilité sociétale
Jour 2 : Questions centrales de responsabilité sociétale
Jour 3 : Questions centrales de responsabilité sociétale (suite) et intégration des pratiques de responsabilité sociétale
Jour 4: Améliorer les performances en matière de responsabilité sociétale
our 5: Examen de certification

Autres Formations

Codes	Formation	Durée	Modes
S01EMSF	ISO 50001 Energy Management System Foundation	2 Jours	self-study
S02EMSLA	ISO 50001 Energy Management System Lead Auditor	5 Jours	self-study
S03EMSLI	ISO 50001 Energy Management System Lead Implementer	5 Jours	self-study
S04MSSDCF	ISO 37101 Management Systems for Sustainable Development in Communities Foundation	2 Jours	self-study
S05MSSDCLA	ISO 37101 Management Systems for Sustainable Development in Communities Lead Auditor	5 Jours	self-study
S06MSSDCLI	ISO 37101 Management Systems for Sustainable Development in Communities Lead Implementer	5 Jours	self-study
S07GSPLM	ISO 20400 Guidelines for Sustainable Procurement Lead Manager	5 Jours	self-study

L'EC-Council (International Council of E-Commerce Consultants) est l'un des leaders mondiaux en matière de certifications en cybersécurité. Reconnue dans plus de 145 pays, cette organisation prestigieuse est à l'origine de formations réputées telles que Certified Ethical Hacker (CEH), Certified Network Defender (CND), ou encore EC-Council Certified Security Analyst (ECSA).

Fondée après les événements du 11 septembre pour répondre aux nouveaux enjeux de cybersécurité, l'EC-Council a pour mission de former des professionnels capables de protéger les systèmes d'information contre les cybermenaces les plus avancées.

Les programmes proposés par l'EC-Council sont conçus en collaboration avec des experts du secteur, et s'appuient sur des scénarios pratiques, des laboratoires virtuels, et une pédagogie orientée compétences. Que ce soit pour les professionnels de l'IT, les administrateurs réseau, les analystes en sécurité ou les consultants en cybersécurité, les certifications EC-Council sont un véritable gage de compétence et de reconnaissance internationale.

CERTIFIED CHIEF INFORMATION SECURITY OFFICER V3

La certification CCISO de l'EC-Council s'adresse aux professionnels souhaitant accéder à des postes de direction en cybersécurité. Ce programme, conçu par des CISOs expérimentés, combine stratégie, leadership, gestion des risques, conformité et sécurité de l'information.

FR | EN **Détails de formation**

Certification Exam Détails

- Format : QCM basés sur des scénarios
- Durée : 2h30
- Note de passage : 60 à 85 %
- Plateforme : portail EC-Council

Pré-requis :

- Minimum 5 ans d'expérience dans au moins 3 des 5 domaines CCISO
- Exonération de formation possible si expérience dans les 5 domaines
- Équivalences via diplômes et certifications

Public :

- CISOs et futurs cadres sécurité
- Directeurs IT / cybersécurité
- Professionnels expérimentés en sécurité

Les 5 domaines clés :

Gouvernance et gestion des risques – Politiques, conformité juridique et stratégie de risque
Contrôles de sécurité et audit – Mise en œuvre, vérification et processus d'audit
Gestion des opérations de sécurité – Supervision quotidienne des activités de cybersécurité
Compétences techniques fondamentales – Principes technologiques, conception de sécurité
Stratégie, finances et gestion des fournisseurs – Budgétisation, achats et alignement métier

Atouts pédagogiques :

Scénarios pratiques et **war games**
Intégration de cadres reconnus : **NIST, GDPR, COBIT, FAIR**
Focus sur les nouvelles technologies : **IA, SOC autonome, cyberdéception**

CERTIFIED CLOUD SECURITY ENGINEER V2

La certification CCSE d'EC-Council forme des professionnels capables de sécuriser des environnements cloud complexes sur AWS, Azure et GCP. Ce programme complet allie théorie, pratiques avancées et laboratoires immersifs pour assurer la maîtrise des défis actuels en cybersécurité cloud.

FR | EN **Détails de formation**

Certification Exam Détails

- Format : QCM basés sur des scénarios
- Durée : 2h30
- Note de passage : 60 à 85 %
- Plateforme : portail EC-Council

Pré-requis :

- Compréhension de base du cloud computing
- Notions fondamentales en sécurité réseau
- Expérience professionnelle en IT ou cybersécurité

Public :

- Ingénieurs cloud & cybersécurité
- Administrateurs IT / réseau
- Professionnels sécurité ou cloud hybrides

Domaines clés abordés :

Architecture cloud sécurisée (multi-tenant, hybride)
Sécurité des plateformes AWS, Azure, GCP
Sécurité des applications (IAM, DevSecOps, CI/CD)
Protection des données & chiffrement
Sécurité des opérations cloud (logs, automatisation)
Réponse aux incidents & forensic cloud
Continuité d'activité et reprise après sinistre
Gouvernance, risques et conformité (GRC)
Normes et législation cloud
Tests d'intrusion cloud

Atouts pédagogiques :

Plus de 85 labs interactifs multi-cloud
Apprentissage par scénarios concrets (incident, IAM, chiffrement…)
Suivi des meilleures pratiques et conformité aux normes (GDPR, ISO, NIST…)

CERTIFIED ETHICAL HACKER V13

La certification CCISO de l'EC-Council s'adresse aux professionnels souhaitant accéder à des postes de direction en cybersécurité. Ce programme, conçu par des CISOs expérimentés, combine stratégie, leadership, gestion des risques, conformité et sécurité de l'information.

FR | EN **Détails de formation**

Certification Exam Détails

- Format : QCM basés sur des scénarios
- Durée : 2h30
- Note de passage : 60 à 85 %
- Plateforme : portail EC-Council

Pré-requis :

- Minimum 5 ans d'expérience dans au moins 3 des 5 domaines CCISO
- Exonération de formation possible si expérience dans les 5 domaines
- Équivalences via diplômes et certifications

Public :

- CISOs et futurs cadres sécurité
- Directeurs IT / cybersécurité
- Professionnels expérimentés en sécurité

Les 5 domaines clés :

Gouvernance et gestion des risques – Politiques, conformité juridique et stratégie de risque
Contrôles de sécurité et audit – Mise en œuvre, vérification et processus d'audit
Gestion des opérations de sécurité – Supervision quotidienne des activités de cybersécurité
Compétences techniques fondamentales – Principes technologiques, conception de sécurité
Stratégie, finances et gestion des fournisseurs – Budgétisation, achats et alignement métier

Atouts pédagogiques :

Scénarios pratiques et **war games**
Intégration de cadres reconnus : **NIST, GDPR, COBIT, FAIR**
Focus sur les nouvelles technologies : **IA, SOC autonome, cyberdéception**

CERTIFIED CLOUD SECURITY ENGINEER V2

La certification **CEH v13** est la référence mondiale en matière de piratage éthique. Propulsée par l'IA, elle forme les professionnels à **penser comme un hacker** pour mieux sécuriser les systèmes. Le programme couvre l'ensemble du cycle d'attaque et introduit l'utilisation de l'IA dans les pratiques de cybersécurité.

FR | EN **Détails de formation**

Certification Exam Détails

Examen théorique :
- Format : QCM 125 question
- Durée : **4h00**
- Note de passage : **60 à 85 %**

Examen pratique :
- 6h de simulation réelle avec 20 défis techniques
- Environnement d'attaque réel
- Obtention du titre **CEH Master**

Pré-requis :

- Bases en réseau, systèmes et sécurité
- Idéal pour profils avec 1 à 2 ans d'expérience en cybersécurité

Public :

- Pentesters, analystes SOC, ingénieurs cybersécurité
- Professionnels IT souhaitant monter en compétence sécurité

Domaines clés abordés :

Reconnaissance
Scanning de vulnérabilités
Prise de contrôle (exploitation)
Maintien d'accès
Effacement des traces
Autres thématiques :
Hacking IA, cloud, IoT, mobile
Attaques web (SQLi, XSS), malware, ingénierie sociale
Cryptographie et contremesures

Atouts pédagogiques :

Plus de 85 labs interactifs multi-cloud
Apprentissage par scénarios concrets (incident, IAM, chiffrement…)
Suivi des meilleures pratiques et conformité aux normes (GDPR, ISO, NIST…)

CERTIFIED NETWORK DEFENDER V3

La certification **CND v3** forme les professionnels à défendre les infrastructures réseau face aux cybermenaces. Elle s'appuie sur une stratégie adaptative et fournit plus de **100 laboratoires pratiques** pour apprendre à **prédire, détecter, protéger et réagir** aux incidents de sécurité.

FR | EN **Détails de formation**

Certification Exam Détails

- Format : QCM basés sur des scénarios
- Durée : **4 heures**
- Plateforme : portail EC-Council
- Accréditations : ANSI ISO 17024, DoD 8140, NCSC UK

Pré-requis :

- Adaptée aux profils juniors ou en transition vers la blue team
- Connaissances de base en réseaux et sécurité informatique

Public :

- Administrateurs et ingénieurs réseau
- Professionnels IT débutants ou en reconversion vers la cybersécurité
- Techniciens SOC, analystes cybersécurité

Domaines clés abordés :

Attaques réseau et stratégies de défense
Sécurité technique et administrative
Sécurité des endpoints (Windows, Linux, Mobile, IoT, Mac)
Sécurité des applications et des données
Sécurité cloud, sans fil et virtuelle
Analyse du trafic réseau et des logs
Réponse aux incidents et investigations forensic
Continuité d'activité et reprise après sinistre
Anticipation des menaces et gestion des risques

Atouts pédagogiques :

Plus de 100 labs pratiques en environnement réel
Intégration de stratégies de défense en profondeur
Basé sur le cadre NIST : **Identifier, Protéger, Détecter, Réagir, Récupérer**
Introduction aux outils modernes : **EDR, XDR, SOAR, UEBA, Zero Trust**
Formation orientée cloud, IoT, mobile, virtualisation, containers

CERTIFIED PENETRATION TESTING PROFESSIONAL VL

La certification **CPENT** d'EC-Council est l'un des programmes les plus complets pour les **pentesters expérimentés**. Elle propose un apprentissage 100 % pratique axé sur les techniques avancées, les environnements complexes (IoT, cloud, Active Directory, SCADA, API) et les outils **alimentés par l'IA**.

FR | EN **Détails de formation**

Certification Exam Détails

Examen théorique :

- Format : **100% pratique** (24h ou 2 x 12h)
- Rapport à remettre sous 7 jours
- 90 % = double titre **CPENT + LPT (Master)**

Pré-requis :

- Bonnes connaissances réseaux, OS, scripting
- Expérience en test d'intrusion et cybersécurité
- CEH ou équivalent recommandé

Public :

- Pentesters avancés et consultants red team
- Professionnels en sécurité applicative
- Ingénieurs cybersécurité offensifs
- Éthical hackers confirmés

Domaines clés abordés :

Préparation et cadrage du test (OSINT)
Ingénierie sociale, tests Web & API
Exploitation AD, Linux, Windows
Reverse engineering, IoT, cloud, SCADA
Techniques avancées (pivot, élévation de privilèges, évasion)
Automatisation avec l'IA (ChatGPT, ShellGPT)
Rédaction de rapport et recommandations

Atouts pédagogiques :

Plus de **110 labs avancés**
5 environnements de simulation réels (AD, IoT, Web, Binaire, CTF)
Focus sur les outils offensifs modernes et la **double pivot**
Apprentissage mixte : labs guidés + autoformation
Scripts, modèles et cheatsheets inclus

EC-COUNCIL CERTIFIED INCIDENT HANDLER V3

La certification **ECIH v3** prépare les professionnels à gérer efficacement les incidents de sécurité (malware, réseau, cloud, email, menaces internes…). Le programme couvre toutes les étapes du processus IH&R (Incident Handling & Response), avec des **labs pratiques** et des outils réels pour s'exercer dans des scénarios complexes.

FR | EN **Détails de formation**

Certification Exam Détails

- Format : QCM - **100 questions**
- Durée : 3 heures
- Plateforme : portail EC-Council
- Accréditations : ISO 17024, DoD 8140, CREST

Pré-requis :

- Expérience minimale de 3 ans en cybersécurité
- Bonnes bases en systèmes, réseaux et sécurité

Public :

- Analystes SOC, gestionnaires d'incidents
- Investigateurs en forensic, CSIRT
- Consultants cybersécurité avec au moins 3 ans d'expérience

Les 5 domaines clés :

1. Processus de gestion des incidents (NIST, MITRE, Kill Chain)
2. Incidents : malware, cloud, email, réseau, applications web
3. Menaces internes, endpoints, IoT, OT
4. Premiers gestes et préparation forensic
5. Collecte de preuves, conformité juridique
6. Eradication, reprise d'activité, post-mortem

Atouts pédagogiques :

Scénarios pratiques et **war games**
Intégration de cadres reconnus : **NIST, GDPR, COBIT, FAIR**
Focus sur les nouvelles technologies : **IA, SOC autonome, cyberdéception**

WEB APPLICATION HACKING AND SECURITY

La formation **WAHS** d'EC-Council propose une immersion pratique dans le piratage et la sécurisation des applications web. Basée sur une approche **Capture-The-Flag (CTF)**, elle couvre les vulnérabilités critiques (SQLi, XSS, CSRF…) et les techniques avancées d'exploitation et de défense.

FR | EN **Détails de formation**

Certification Exam Détails

Examen pratique de 6h, surveillé à distance
Niveaux :
- ⩾ **60 %** : Web Application Associate
- ⩾ **75 %** : Web Application Professional
- ⩾ **90 %** : Web Application Expert

Accès à l'espace examen : **30 jours**

Pré-requis :

- Bases en développement web, HTTP, et sécurité
- Connaissance de CEH, CND ou expérience en test web recommandée

Public :

- Pentesters et hackers éthiques
- Ingénieurs sécurité applicative
- Auditeurs red team, développeurs sécurité
- Répondants aux incidents

Domaines clés abordés :

1. Tests d'intrusion web avancés
2 SQL Injection, XSS, CSRF
3 Mauvaises configurations, failles d'accès, LFI/RFI
4 Téléversements arbitraires, exécutions de code
5 Clickjacking, manipulation de cookies et en-têtes
6 Vulnérabilités OWASP Top 10

Atouts pédagogiques :

Défis "Break the Code" en mode CTF
60 heures de contenu guidé
20+ laboratoires réels
Évolution par niveau : débutant → expert
Classement en temps réel par performance

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
CASE .NET	Sécurité des applications	Intermédiaire	Développeurs .NET, ingénieurs QA	E-learning	OWASP, DevSecOps, SDLC sécurisé
CASE Java	Sécurité des applications	Intermédiaire	Développeurs Java, auditeurs	E-learning	Approche SDLC, tests & intégration continue
Certified Blockchain Professional v2 (CBP)	Blockchain & sécurité	Intermédiaire	Dév, architectes blockchain, IT	E-learning	Concepts cryptos, smart contracts, sécurité blockchain
Certified Cybersecurity Technician (CCT)	Fondamentaux cybersécurité	Débutant	Nouveaux entrants, techniciens IT	E-learning + Labs	Idéal pour certifications de base, multitechno

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
Certified in Advanced Penetration Testing (APT)	Pentest avancé	Avancé	Pentesters, Red Team	Labs pratiques	Lab intensif multi-vectoriel, post-CPENT
Certified Secure Computer User (CSCU)	Sécurité utilisateur	Débutant	Tout public, employés non-tech	E-learning	Sécurité email, social engineering, navigation
Certified SOC Analyst (CSA)	Opérations SOC	Intermédiaire	Analystes SOC, niveau 1 & 2	Classe virtuelle	Détection des incidents, logs, SIEM
Certified Threat Intelligence Analyst (CTIA)	Threat Intel	Avancé	Analystes CTI, investigateurs cyber	E-learning	OSINT, sources dark web, attribution d'attaque

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
Cloud Security Essentials (CSE)	Sécurité cloud	Débutant	Administrateurs cloud, juniors IT	E-learning	Cloud concepts, sécurité AWS/Azure, IAM
Computer Hacking Forensic Investigator (CHFI)	Forensic & enquête numérique	Avancé	Enquêteurs, juristes, police tech	E-learning	Analyses post-attaque, légalité, chaînes de preuve
DevSecOps Essentials (DSE)	DevSecOps	Débutant	Dév & ingénieurs DevOps	E-learning	Intégration de la sécurité dans CI/CD
Digital Forensics Essentials (DFE)	Forensic de base	Débutant	Étudiants, profils IT curieux	E-learning	Introduction aux outils forensic & process IR

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
EC-Council Certified DevSecOps Engineer (ECDE)	DevSecOps avancé	Intermédiaire	Ingénieurs sécurité CI/CD	E-learning	Intégration sécurité dans pipelines automatisés
EC-Council Certified Encryption Specialist (ECES)	Cryptographie	Intermédiaire	Dév, admins réseau, compliance	E-learning	Algorithmes symétriques, PKI, hash
EC-Council Certified Security Analyst (ECSA v10)	Pentest avancé	Avancé	Pentesters certifiés CEH	E-learning + labs	Préparation à CPENT, reporting & standards
EC-Council Certified Security Specialist (ECSS v10)	Sécurité IT globale	Débutant	Étudiants, juniors IT	E-learning	Réseaux, OS, sécurité des infos

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
EC-Council Certified Security Specialist (ECSS v10)	Sécurité IT globale	Débutant	Étudiants, juniors IT	E-learning	Réseaux, OS, sécurité des infos
EC-Council Disaster Recovery Professional (EDRP)	Continuité d'activité	Intermédiaire	DSI, RSSI, managers risque	E-learning	BCP, DRP, analyse d'impact, test de reprise
Ethical Hacking Essentials (EHE)	Hacking éthique	Débutant	Étudiants, profils curieux	E-learning	Initiation au CEH, scénarios ludiques

Titre de la formation	Domaine	Niveau	Public cible	Format	Remarques clés
IoT Security Essentials (ISE)	IoT & objets connectés	Débutant	Techs IoT, cybersécurité	E-learning	Menaces IoT, architecture sécurisée
LPT (Master)	Pentest expert	Expert	Red Team, post-CPENT	Cyber range	Certification elite, scénarios 24h
Network Defense Essentials (NDE)	Défense réseau	Débutant	Étudiants IT / réseaux	E-learning	Défense périmétrique, protocoles sécurisés
SOC Essentials (SCE)	SOC et détection	Débutant	Juniors analystes SOC	E-learning	Logs, détection de compromission
Threat Intelligence Essentials (TIE)	Cyber renseignement	Débutant	Analystes, étudiants cybersécurité	E-learning	Introduction aux IOC, TTPs, outils OSINT

Nos Partenaires

SUPINFO

TELECOM ParisTech

eni

CLUBEBIOS

UNIVERSITE DE MONDIAPOLIS

cegos Beyond knowledge

skillsoft global knowledge

ingésup

Orange Cyberdefense

ORDRE NATIONAL DES EXPERTS INTERNATIONAUX

iprec Formations informatiques depuis 1971

ITESCIA L'ÉCOLE DU E-MANAGEMENT

EduGroupe Accompagner pour réussir

ipi INFORMATIQUE ET NUMÉRIQUE UNE ÉCOLE DU GROUPE IGS

Togocom

H3 Hitema

Conditions Générales de Vente des Formations OGSBC

1. Modalités de Formation

OGSBC propose plusieurs modes de formation pour répondre aux besoins de ses clients :
Formation en présentiel : Sessions organisées dans nos locaux ou dans un lieu dédié, avec un formateur certifié.
E-learning : Accès à une plateforme en ligne pour suivre des modules de formation à son rythme.
Classes virtuelles : Sessions de formation en direct, dispensées par un formateur via une plateforme de visioconférence.
Self-study : Accès à des ressources pédagogiques (documents, vidéos, quiz) pour un apprentissage autonome.

2. Inscription et Paiement

Inscription : L'inscription à une formation est validée dès réception du formulaire d'inscription dûment complété et signé, accompagné du règlement ou d'une preuve de paiement.
Paiement : Le paiement doit être effectué intégralement avant l'accès à la formation, sauf accord préalable pour un échelonnement. Les modes de paiement acceptés sont : virement bancaire, carte de crédit ou autres moyens spécifiés sur le site.
Accès aux formations :
Pour les formations en e-learning et self-study, l'accès aux ressources sera activé sous 48 heures après validation du paiement.
Pour les classes virtuelles et les formations en présentiel, un email de confirmation avec les détails pratiques sera envoyé après validation de l'inscription.

3. Annulation et Remboursement

Annulation par le participant :
Pour les formations en présentiel et classes virtuelles :
Annulation plus de 15 jours avant le début de la formation : remboursement intégral.
Annulation entre 15 et 7 jours avant la formation : 50% du montant sera remboursé.
Annulation moins de 7 jours avant la formation : aucun remboursement.
Pour les formations en e-learning et self-study : Aucun remboursement après activation de l'accès aux ressources.
Annulation par OGSBC : En cas d'annulation de la formation par OGSBC, un remboursement intégral sera effectué ou une proposition de report à une date ultérieure sera faite.

4. Report de Formation

Les participants peuvent demander un report de leur inscription à une session ultérieure, sous réserve de disponibilité et sous condition que la demande soit faite au moins 7 jours avant la date initiale de la formation (applicable uniquement aux formations en présentiel et classes virtuelles).

5. Accès aux Supports de Formation

Les supports de cours seront accessibles via notre plateforme en ligne après réception du paiement complet. Les participants recevront un identifiant et un mot de passe personnels pour accéder aux ressources.
Pour les formations en e-learning et self-study, l'accès aux ressources est valable pour une durée limitée (par exemple, 6 mois ou 1 an), sauf indication contraire.

6. Certification

La délivrance des certifications est soumise à la réussite des examens correspondants. OGSBC n'est pas responsable des échecs aux examens et ne garantit pas l'obtention des certifications.
Pour les formations en self-study, les participants doivent s'inscrire séparément aux examens de certification auprès des organismes partenaires (EC-Council, PECB, etc.).

7. Propriété Intellectuelle

Tout le matériel de formation fourni est la propriété intellectuelle d'OGSBC ou de ses partenaires. La reproduction, distribution ou utilisation commerciale sans autorisation écrite est strictement interdite.

9. Modifications des Conditions

OGSBC se réserve le droit de modifier ces conditions de vente à tout moment. Les conditions applicables seront celles en vigueur au moment de l'inscription.

10. Loi Applicable et Juridiction

Les présentes conditions sont régies par la loi en vigueur dans le pays où OGSBC est établi. Tout litige relatif à l'interprétation ou à l'exécution de ces conditions sera soumis aux tribunaux compétents de ce pays.

8. Limitation de Responsabilité

OGSBC ne pourra être tenu responsable des dommages indirects ou des pertes de données résultant de la participation à nos formations.
Pour les formations en e-learning et classes virtuelles, OGSBC ne garantit pas un accès ininterrompu à la plateforme en raison de problèmes techniques indépendants de sa volonté (maintenance, panne de serveur, etc.).

OG Security Business Consulting

BULLETIN D'INSCRIPTION

à nous renvoyer scanné par courriel à **contact@ogsbc.ma**

FORMATION CHOISIE :

N°	Intitule de la formation :	Formule choisie : (Cochez la case qui correspond à votre choix.)		
		E-learning	Self-study	Classe virtuelle
1				
2				
3				
4				

INFORMATIONS SUR LE CANDIDAT :

Nom et prénom : .....

Fonction : .....

Adresse : .....

Pays : .....

Email : ..... **Tél :**..... **GSM :** .....

Si vous avez déjà un compte PECB, veuillez indiquer votre ID (sinon, laisser vide) : .....

COUT DE LA FORMATION :

A remplir selon les informations que vous avez reçu par email suite à votre pré-inscription sur notre site.

REDUCTION : Si vous avez un code de réduction en cours de validité, veuillez l'inscrire et appliquer la réduction)	Code réduction :	**OGSCYBER**
	Prix initial de la formation :	
	Taux de réduction : **Net à payer :**	

CONDITIONS GÉNÉRALES DE VENTE :

CONDITIONS D'INSCRIPTION

Votre inscription à une formation n'est définitive qu'après réception du présent bulletin d'inscription dument remplit, signé accompagné de l'ordre de virement équivalent aux frais de participation à la formation.

Règlement reçu par virement bancaire sur le compte de Monsieur Jamal SAAD :

- En Dirham N° 190 780 2111115369780000 22 chez Banque Populaire – LAHJAJMA, dont le siège social est à bd de Bourgogne rue Jaâfar Ibn Habib Quartier bourgogne Casablanca - Maroc.

Code SWIFT : BCPOMAMC

CONDITIONS DE SUBSTITUTION, D'ANNULATION ET DE REMBOURSEMENT

Les substitutions de participants ne sont plus acceptées 15 jours avant le début de la formation.

Si une annulation nous parvient 30 jours ouvrables avant le début de la formation, les frais sont remboursés intégralement.
Sinon, aucun remboursement ne sera effectué.

Fait à .....le.....

Signature :

J'ai pris connaissance des conditions d'inscription et d'annulation ci-dessus, et j'accepte les Conditions Généralesde Vente d'OGSBC

BULLETIN D'INSCRIPTION

CONDITIONS GÉNÉRALES

''Pour pourvoir faire de la veille stratégique et de l'intelligence économique, il faut très certainement repenser nos mesures cyber et identifier le périmètre critique de nos organisations comme un véritable territoire à sécuriser''

POUR NOUS JOINDRE:

OGSBC

Rue Ahmed SIJILMASSI numéro 23,
Tanger, 90000 - Maroc
Tél (+212) 7 08 08 87 87

(+33) 6 36 36 36 46

E-mail: contact@ogsbc.ma

www.ogsbc.ma