SECUREDSYS INSTITUTE

CATALOGUE DE FORMATION

2026 - 2027

NOS PARTENAIRES

FDFP
Fonds de Développement de la Formation Professionnelle

ISACA
Accredited Partner

PeopleCert
All talents, certified.

PECB

SOMMAIRE

Dans un monde où les menaces se font de plus en plus sophistiquées et la transformation digitale s'accélère, la gestion des risques et la cybersécurité sont devenues des enjeux majeurs pour toutes les organisations. Que vous soyez une PME, une grande entreprise ou une institution publique, vous devez protéger vos données, vos systèmes et votre réputation. Mais il est également essentiel de maîtriser la gestion de projets et l'amélioration des processus pour assurer la compétitivité et la pérennité de votre entreprise.

C'est dans cette optique que notre cabinet de formation a conçu un catalogue de formations spécialisées pour vous aider à développer les compétences essentielles dans ces domaines. Nos experts, reconnus pour leur expérience et leur pédagogie, vous transmettront les connaissances et les outils nécessaires pour anticiper, identifier et gérer les risques mettre en place une stratégie de cybersécurité efficace, protéger vos données sensibles, piloter vos projets avec succès et optimiser vos processus métiers.

Notre offre de formation couvre un large éventail de thématiques :

- ***Gestion des risques*** *: identification, évaluation, traitement et suivi des risques, conformité réglementaire, audit interne.*
- ***Gestion des projets*** *: planification, exécution, suivi et contrôle de projets, gestion des ressources, gestion des risques projet, méthodologies agiles.*
- ***Cybersécurité*** *: protection des données, sécurité des réseaux, gestion des identités et des accès, réponse aux incidents, sensibilisation des utilisateurs.*
- ***Excellence opérationnelle*** *: analyse des processus existants, identification des points faibles, conception et mise en place de processus optimisés, Lean Management, Six Sigma.*

Nos formations sont conçues pour répondre à vos besoins spécifiques :

- ***Formations inter-entreprises*** *: partagez vos expériences avec d'autres professionnels et élargissez votre réseau.*
- ***Formations intra-entreprises*** *: personnalisées pour répondre aux enjeux spécifiques de votre organisation.*
- ***Formations à distance*** *: apprenez à votre rythme et depuis où vous le souhaitez.*

En choisissant notre cabinet, vous bénéficiez de :

- ***Une expertise reconnue*** *: nos formateurs sont des experts dans leur domaine.*
- ***Des contenus de qualité*** *: nos formations sont basées sur les meilleures pratiques et les dernières tendances.*
- ***Une approche pédagogique innovante*** *: nous privilégions l'interactivité et la mise en pratique.*
- ***Un accompagnement personnalisé*** *: nous sommes à votre écoute pour vous conseiller et vous orienter.*

N'attendez plus, investissez dans votre avenir en vous formant à la gestion des risques, à la cybersécurité, à la gestion de projets et à l'amélioration des processus.
Consultez notre catalogue de formations et contactez-nous pour en savoir plus.

Ensemble, construisons un avenir plus sûr, plus performant et plus serein.

L'équipe de SECUREDSYS

Présentation du cabinet

Fondée en 2021 par un groupe de passionnés accompagné d'experts aux profils complémentaires**, SECUREDSYS INSTITUTE** est la marque de l'entreprise **SECURED SYSTEMS INTERNATIONAL** dédiée à la formation professionnelle continue et à la certification des personnes dans les domaines de la gouvernance, le management d'entreprise, l'audit, la gestion des risques, la sécurité de l'information, la Cybersécurité, la Qualité, la Santé, l'Hygiène et la sécurité environnementale.

SECUREDSYS INSTITUTE propose un éventail de formations spécifiquement conçues pour sensibiliser les managers et les décideurs aux enjeux de la transformation numérique, tout en leur donnant des clés concrètes de compréhension et des éléments de sécurité informatique.

SECUREDSYS INSTITUTE est habilité pour délivrer d'une part les cursus de formation, mais aussi possède les accréditations permettant de valider le niveau d'expertise des candidats en proposant le passage des examens internationaux de certification.

SECUREDSYS INSTITUTE s'appuie sur un réseau d'experts reconnus dans leur domaine de compétences alliant approche pédagogique, expérience terrain et savoir-faire professionnel pour la satisfaction assurée des Stagiaires.

SECUREDSYS INSTITUTE crée de la valeur en sensibilisant aux enjeux de demain à travers un service de veille pédagogique performant et efficace.

Mission : Contribuer à la performance et à la création de la valeur de nos clients par l'accompagnement du capital humain à la maîtrise des enjeux et risques de la digitalisation et la globalisation.

Objectif : Devenir une référence Africaine pour le développement des compétences humaines et organisationnelles, en s'appuyant sur les standards internationaux, des expertises reconnues et une démarche qualité afin de se différencier de la concurrence et consolider sa position de façon durable.

Où nous trouver ?

BUREAU D'ABIDJAN
ABIDJAN, COCODY LES 2 Plateaux
Rue des OSCARS
18 BP M440 ABIDJAN 18
+225 2722280668 / +225 0798419519
contact@securedsys.net / formation@securedsys.net
www.securedsys.net

BUREAU DE PARIS
23 Rue Hélène, 78260 Achères
+33 631 664 974

BUREAU DE MONTREAL
1338 Rue des Calèches G3K0M8, Québec
+1 418 264 5120

6 raisons de nous choisir

Professionnalisme

SECUREDSYS INSTITUTE se distingue par son professionnalisme et son engagement envers l'excellence. Nos formations sont conçues avec rigueur, en s'appuyant sur les meilleures pratiques et les standards internationaux. Chaque programme est structuré pour offrir un apprentissage de qualité, assuré par des formateurs expérimentés et certifiés.

Qualité

Nous appliquons une démarche d'amélioration continue basée sur l'écoute des participants, l'évaluation des performances et l'optimisation constante des contenus. Nos certifications et accréditations témoignent de notre engagement à offrir des formations fiables, pertinentes et immédiatement applicables, renforçant ainsi la compétence et la compétitivité de nos apprenants.

Réactivité

Nous anticipons les besoins en formation, adaptons nos contenus en temps réel et garantissons une prise en charge rapide et efficace. Notre approche agile nous permet d'accompagner les professionnels avec des solutions pédagogiques innovantes et performantes, assurant ainsi leur montée en compétences.

Expertise

Grâce à une équipe d'experts qualifiés et à des méthodologies éprouvées, nous accompagnons les entreprises dans l'optimisation de leurs processus et le renforcement de leur sécurité. Notre approche allie innovation, rigueur et conformité aux standards internationaux, garantissant des solutions adaptées aux défis actuels et futurs des organisations.

Certification

Grâce à notre expertise et à nos partenariats stratégiques, nous proposons plusieurs certifications adaptées aux exigences du marché dans des domaines clés tels que la cybersécurité, la gestion des risques, la conformité et le management des systèmes d'information et bien d'autres...

Accréditation

Nos accréditations témoignent de notre engagement à offrir des formations fiables, pertinentes, conforme aux exigences des nos partenaires et respectant les règles de propriété intellectuelle. Nos supports sont régulièrement mis à jour afin d'intégrer les nouveautés du métier, nos formateurs sont accrédités par les partenaires et un kit de formation officiel est mis à la disposition des apprenants

Nos partenariats et accréditations

Le Fonds de Développement de la Formation Professionnelle (FDFP) est l'organisme de conception, d'organisation et de gestion de la formation professionnelle mise en place par le gouvernement Ivoirien pour faciliter l'acquisition et le transfert de compétences.
Il oriente, impulse et met en œuvre la politique de formation de la formation professionnelle continue et l'Apprentissage en Côte d'Ivoire.

PECB (Professional Evaluation and Certification Board) est un organisme de formation qui offre des services de formation, de certification et des programmes de certificats aux personnes dans plusieurs disciplines conformément à des normes rigoureuses et reconnues internationalement parmi lesquelles l'ISO (International Standard Organisation).

PeopleCert est un leader mondial de la formation et de la certification professionnelle, proposant des cadres de bonnes pratiques et des certifications reconnues à l'international. Présente dans plus de 200 pays, son portefeuille incluant ITIL®, PRINCE2®, DevOps Institute® et LANGUAGECERT®. Accompagne le développement des compétences et la performance des organisations à l'échelle mondiale.

SECUREDSYS EST ACCRÉDITÉ ATO PAR ISACA

SECUREDSYS INSTITUTE a obtenu son accréditation en tant que centre de formation ISACA en Côte d'Ivoire (Premier cabinet de formation installé en Afrique Subsaharienne francophone). Cette reconnaissance témoigne de notre engagement envers l'excellence et de notre expertise dans les domaines de la gouvernance, de la sécurité et de l'audit des systèmes d'information. Vous pouvez vous former et préparer les certifications délivrées par ISACA en français directement dans notre centre de formation à Abidjan ou en ligne !!!

ISACA (Information Systems Audit and Control Association) est un organisme international qui propose des services de formation, de certification et des programmes de développement professionnel dans les domaines de l'audit, du contrôle, de la sécurité, de la gestion des risques et de la gouvernance des systèmes d'information, en conformité avec des normes mondialement reconnues.

Notre assurance qualité

SECUREDSYS INSTITUTE a mis en place un système de management de la qualité reposant sur une approche rigoureuse et proactive pour garantir la satisfaction de nos principales parties prenantes.
Cette satisfaction est le résultat d'un processus structuré qui allie remise en question permanente, outils de mesure performants et une amélioration continue de l'ensemble de nos prestations.

Nous évaluons sans la qualité de nos prestations à travers des outils spécifiques tels que :

Des évaluations à chaud

Des évaluations à chaud réalisées immédiatement après chaque session pour recueillir vos impressions sur le contenu, la pédagogie, et l'environnement de formation.

Des évaluations à froid

Des évaluations à froid effectuées plusieurs semaines après la formation pour mesurer l'impact concret des compétences acquises sur votre activité professionnelle

Des Audits internes

Des audits internes réguliers pour contrôler la conformité de nos programmes et de nos pratiques par rapport aux normes internationales

Analyse des retours et la mesure des kpi

Des indicateurs clés de performance (KPI) pour analyser les retours de satisfaction, les taux de réussite aux certifications et le niveau d'engagement des stagiaires.

Ces données, croisées et analysées par notre équipe, nous permettent d'identifier avec précision les axes d'amélioration nécessaires. Nous adaptons ainsi nos méthodes pédagogiques, enrichissons nos supports de formation et modernisons nos infrastructures pour garantir un environnement optimal.
Les *retours des clients, qu'ils soient spontanés ou sollicités, sont au cœur de notre démarche. Ils nous permettent d'innover et d'aller au-delà des standards habituels en anticipant vos attentes. SECUREDSYS INSTITUTE s'engage à offrir bien plus qu'une simple formation : une expérience enrichissante, alignée sur vos objectifs professionnels et soutenue par une équipe à l'écoute des besoins de nos clients.*

Notre expertise

SECUREDSYS INSTITUTE *dispose d'une expertise solide bâtie sur des années d'expérience, nous offrons des parcours de formation sur mesure pour répondre aux besoins spécifiques des entreprises et des professionnels dans un environnement technologique en constante évolution.*

Notre expertise repose sur :

Des formateurs certifiés *: Experts dans leurs domaines, nos formateurs combinent des connaissances théoriques approfondies et une expérience terrain avérée pour offrir des formations concrètes, pertinentes et adaptées aux réalités opérationnelles.*

Des programmes alignés sur les normes internationales *: Nos contenus de formation sont conçus en conformité avec les standards mondialement reconnus, tels que l'ISO, COBIT, NIST, et autres référentiels incontournables.*

Une spécialisation sectorielle *: Nous intervenons dans des secteurs variés, notamment la finance, l'énergie, les télécommunications et l'industrie, en proposant des solutions adaptées à leurs spécificités et leurs contraintes.*

Solutions personnalisées *: Nous analysons vos besoins spécifiques pour vous proposer des parcours de formation et d'accompagnement sur mesure, favorisant l'acquisition de compétences immédiatement applicables.*

Innovations pédagogiques *: Nos formations intègrent des outils modernes (simulations, ateliers pratiques, études de cas) pour maximiser l'engagement et l'apprentissage des participants.*

Certifications reconnues *: En tant que partenaire de certification agréé, nous vous aidons à valoriser vos compétences par des diplômes et accréditations à forte valeur ajoutée sur le marché.*

Une vision tournée vers l'avenir *: SECUREDSYS INSTITUTE s'engage à accompagner les professionnels et les organisations dans la maîtrise des défis de demain en matière de cybersécurité, de résilience informatique et de conformité réglementaire.*

Formats des sessions

1 Les formations inter-entreprises ou sessions ouvertes

Ce sont des sessions planifiées dans notre calendrier laissant la possibilité aux professionnels intéressés de s'inscrire.
Les avantages :

- *Vous pouvez vous former ou faire former un collaborateur seul, en choisissant la formation la plus adaptée à son niveau.*
- *La présence de salariés de diverses entreprises favorise le partage d'expérience entre les stagiaires, en particulier entre cabinets d'experts comptables et praticiens d'entreprises.*
- *Vous pouvez planifier la formation à partir du calendrier existant, en fonction de la disponibilité de chacun et sans gérer des agendas croisés complexes.*
- *Vous n'avez pas à vous soucier de mettre à disposition une salle.*

2 Les sessions fermées ou formations intra-entreprise

Elles rassemblent les collaborateurs d'une entreprise concernée par un thème de formation. La date, le lieu et les modules de formation sont définis de commun accord avec l'entreprise concernée.
Les avantages :

- *Des modules adaptés à votre problématique, en fonction des besoins de l'entreprise et du niveau des stagiaires.*
- *Les formations 'intra' favorisent la cohésion d'équipe et la compréhension commune des contraintes et process internes associés au sujet.*
- *Vous choisissez avec nous la date et le lieu de la formation.*
- *Le coût peut être plus intéressant, à partir de 4 ou 5 participants, en « intra » plutôt qu'en « inter ».*

La plupart de nos formations « inter » peuvent être également proposées en « intra »

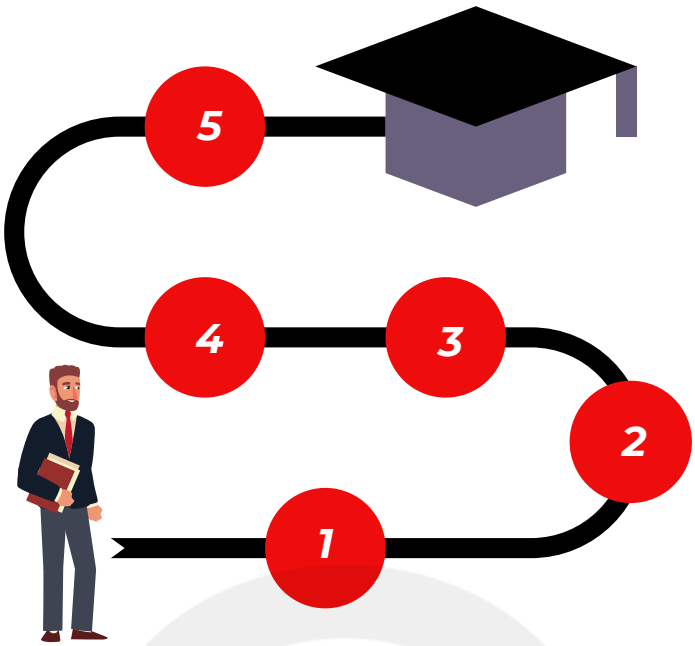
3 Les classes virtuelles ou distancielles

Elles permettent de participer aux formations en direct avec le formateur, à travers son écran et des outils de visio-conférence ou autre accessibles à tous.
Les avantages :

- *Vous suivez la formation depuis votre ordinateur chez vous ou au bureau, à date et heure fixée à l'avance.*
- *Les interactions avec le formateur et les autres participants sont conservées (mode replay disponible).*
- *Pas de contraintes de déplacement, ni de coûts associés.*
- *La formation a été spécialement construite pour cette modalité.*

Nos formations « inter » et « intra » sont traditionnellement proposées en « présentiel », c'est à dire en présence physique du formateur et des stagiaires, Cependant nous adaptons toutes nos formules aux besoins du client.

PARCOURS DE FORMATION



1 ***Identification de la formation***

Le client identifie une formation dans notre catalogue plus de 250 formations organisé en plusieurs domaines.

2 ***Prise de contact et alignement***

Le client nous contacte pour avoir plus de détails sur la formation choisie et le conseil d'un de nos experts pour l'évaluation de l'adéquation de celle-ci avec ses besoins personnels et professionels.

3 ***Inscription à la session***

Le client recoit une offre financière correspondant à son besoin, accompagné d'une fiche d'inscription.
NOTE : Il est important de nous retourner la fiche d'inscription dûment remplie et de s'acquitter des frais obligatoires mentionnés dans l'offre pour finaliser ses démarches d'inscription.

4 ***Organisation de la formation***

La session est organisée et animée dans les conditions du contrat. A l'issue de celle-çi, nous procedons à une évaluation à chaud des notions apprises et une attestation de formation est délivrée à chaque participant.

5 ***Accompagnement sur mesure***

Pour chacunes de nos formations, nous mettons en place un accompagnement de 3 mois par le formateur afin de favoriser la mise en pratique des compétences et conaissances acquises. Dans le cadre des formations certifiantes, cet accompagnement vise à permettre une préparation intensive afin maximiser les chances de réussite aux examens de certifications.

La liste des formations de ce catalogue n'ést pas exhaustive. N'hesitez pas à nous contacter pour tous vos besoins de formation, d'accompagnement, dévellopement de compétences n'y figurant pas.

NOS DOMAINES DE FORMATION

- Sécurité de l'Information & Cybersécurité
- Management d'Entreprise et Gestion des Projets
- Gouvernance, Audit et Gestion des Risques
- Qualité, Hygiène, Sureté et Environnement
- Technologies de l'Information & de la Communication
- Normes ISO et Conformité


APC
Schneider Electric
NetApp
intel
DELL

CISM® : CERTIFIED INFORMATION SECURITY MANAGER

La certification CISM, délivrée par l'ISACA (Information Systems Audit and Control Association), est une certification professionnelle mondialement reconnue qui atteste de compétences avancées en management de la sécurité de l'information. Elle s'adresse aux professionnels qui gèrent, conçoivent, supervisent et évaluent la sécurité de l'information d'une entreprise, comme les responsables de la sécurité des systèmes d'information (RSSI), les consultants en sécurité et les auditeurs en sécurité.

5 jours

code : CISM

CISM Certified Information Security Manager. An ISACA Certification

Objectifs

- Comprendre les 4 domaines de la gestion de la sécurité de l'information selon les exigences du CISM ;
- Maîtriser le vocabulaire et les modalités de l'examen de certification ;
- Découvrir l'ensemble des normes et procédures applicables au management de la sécurité de l'information ;
- Se préparer et réussir l'examen officiel CISM® (Certified Information Security Manager).

Public Cible

- Administrateur réseaux - télécoms
- Administrateur système
- Ingénieur système
- Ingénieur réseaux - télécoms
- Auditeur interne / externe
- Manager
- Professionnels de l'informatique, en particulier les cadres chargés de gérer la sécurité de l'information

Prérequis

- Une expérience professionnelle de 5 ans* minimum dans le domaine de la gestion de la sécurité de l'information, dont au moins 3 ans dans (la gouvernance de la sécurité de l'information ; la gestion des risques liés à l'information et la conformité ; le développement et la gestion des programmes de sécurité de l'information la gestion des incidents de sécurité de l'information).

**Note : si vous êtes titulaire d'un diplôme universitaire en sécurité de l'information (par exemple, un master en cybersécurité) ou de certaines certifications reconnues par l'ISACA (par exemple, CISSP et CISA), vous bénéficierez d'une dispense d'expérience d'un an.*

- Une bonne compréhension des infrastructures réseau et des notions de cryptographie.
- Savoir lire et écrire l'anglais technique pour comprendre les supports de cours et passer l'examen officiel (la formation est dispensée en français).

PROGRAMME

Module 1 : gouvernance de la sécurité de l'information

- Concilier les stratégies de sécurité de l'information avec la stratégie de l'organisation.
- Développer une politique de sécurité de l'information performante.
- Répartir les rôles et les responsabilités au sein de la gouvernance.
- Réaliser un audit, information et communication autour de la gouvernance de la sécurité.

Module 2 : gestion des risques de l'information

- Mettre en place une approche systématique et analytique et un processus continu de gestion des risques.
- Identifier, analyser et évaluer les risques.
- Définir des stratégies de traitement des risques.
- Mettre en place une communication effective autour de la gestion des risques.

Module 3 : développement et gestion d'un plan de sécurité IT

- Comprendre l'architecture de la sécurité de l'information.
- Comprendre la méthodologie et les pratiques pour mettre en place des mesures de sécurité.
- Gérer les contrats et les prérequis de la sécurité de l'information.
- Utiliser les métriques et évaluer la performance de la sécurité.

Module 4 : gestion des incidents de la sécurité de l'information

- Comprendre le fonctionnement du plan de gestion des incidents de sécurité.
- Connaître les pratiques et techniques de la gestion des incidents de sécurité.
- Avoir une méthode de classification.
- Connaître les processus de notification et d'escalade.
- Détecter et analyser les incidents.

Module 5 : préparation à l'examen CISM

- Présentation des types de questions de l'examen.
- Passage d'un examen blanc complet (correction détaillée et analyse des résultats).
- Conseils et stratégies pour réussir l'examen (gestion du temps, techniques de lecture des questions et gestion du stress).

CISSP® : CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

La formation CISSP® (Certified Information Systems Security Professional), s'adresse aux professionnels possédant un haut niveau d'expertise en sécurité informatique. Elle est notamment adaptée pour les responsables de la sécurité des systèmes d'information (RSSI) et pour les directeurs des systèmes d'information (DSI). Toutefois, cette formation certifiante est utile dans plusieurs métiers, puisqu'elle aborde des compétences spécifiques dans le domaine de la cybersécurité.

5 jours

code : CISSP

Objectifs

- Connaître les 8 domaines du Common Body of Knowledge défini par l'(ISC)²;
- Acquérir des compétences et des connaissances avancées en sécurité des systèmes d'information et en gestion des risques informatique ;
- Passer l'examen officiel CISSP® et décrocher votre certification.

Public Cible

- Administrateur système
- Ingénieur système
- Directeur des Systèmes d'Information (DSI)
- Responsable sécurité informatique
- Analyste cybersécurité
- Auditeur interne / externe

Prérequis

- Compétences fondamentales sur les réseaux, les systèmes d'exploitation et sur les pratiques de la sécurité de l'information ;
- Notions élémentaires sur les normes d'audit et les normes internationales de gestion de continuité des activités.
- Savoir lire et comprendre l'anglais afin de consulter les supports de cours et passer l'examen CISSP®.

PROGRAMME

Domaine 1 : la sécurité et la gestion des risques

Domaine 2 : la sécurité des actifs

Domaine 3 : l'architecture et l'ingénierie de sécurité

Domaine 4 : la sécurité des communications et des réseaux

Domaine 5 : la gestion des identités et des accès

Domaine 6 : l'évaluation et les tests de sécurité

Domaine 7 : les opérations de sécurité

Domaine 8 : la sécurité du développement logiciel

ISO/IEC 27001 : LEAD IMPLEMENTER

L'objectif d'un système de gestion de la sécurité de l'information (SMSI) est d'implémenter des mesures qui permettent une réduction, voire une suppression des différentes menaces dans une organisation afin de favoriser la continuité de l'activité, la protection des actifs informationnels et la confiance du client. La norme ISO 27001 version 2022 décrit sous forme d'exigences, un ensemble de bonnes pratiques organisationnelles, techniques et des points de contrôle à mettre en place pour s'assurer de la pertinence du SMSI.

5 jours

code : ISO27001LI

Objectifs

- Distinguer la relation entre la norme ISO 27001 et la norme ISO 27002 puis les autres règlementations associées ;
- Maîtriser les concepts, pratiques et techniques pour implémenter et gérer un Système de Management de la Sécurité de l'Information (SMSI) ;
- Appliquer les directives de la norme ISO 27001 dans un cas particulier au sein d'une organisation ;
- Accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la mise à jour du SMSI ;
- Conseiller une organisation sur les pratiques relatives au SMSI

Public Cible

- Administrateur système
- Architecte informatique / SI
- Ingénieur système
- Auditeur interne / externe
- Chef de projet / Responsable de projet
- Contrôleur de gestion
- Directeur des Systèmes d'Information (DSI)

Prérequis

- Etre impliqué dans la sécurité des systèmes d'information ;
- Connaitre les principes fondamentaux de la norme ISO 27001 et son application.

PROGRAMME

Jour 1 : Introduction à la norme ISO/IEC 27001 et démarrage de la mise en œuvre d'un SMSI

- Introduction au système de management et de l'approche processus ;
- Présentation des normes ISO 27001:2022, ISO 27002:2013 et ISO 27003:2017
- Les principes fondamentaux de la sécurité de l'information ;
- L'analyse préliminaire et l'établissement du niveau de maturité d'un système de management de la sécurité de l'information existant basée sur la norme ISO 21827:2008 ;
- La rédaction de la rentabilité et la planification de la mise en œuvre d'un SMSI.

Jour 2 : Plan de mise en œuvre d'un SMSI

- Définition de la portée d'un SMSI ;
- Implémentation d'un SMSI et politiques de sécurité de l'information ;
- Sélection de l'approche et de la méthodologie d'évaluation des risques ;
- La gestion des risques : l'identification, l'analyse et le traitement des risques (en s'inspirant des orientations de la norme ISO 27005:2011)
- La rédaction de la Déclaration de l'Applicabilité (DdA).

Jour 3 : Mise en œuvre du SMSI

- la mise en œuvre du cadre de gestion documentaire ;
- la conception des mesures et les procédures de rédaction ;
- la mise en œuvre des mesures ;
- le développement d'un programme de formation, de sensibilisation et de communication sur la sécurité de l'information
- la gestion des incidents (fondée sur la norme ISO 27035:2016) ;
- la gestion des opérations d'un SMSI.

Jour 4 et 5 : Suivi, amélioration continue et préparation à l'audit de certification du SMSI

- le contrôle et le suivi du SMSI ;
- l'élaboration de mesures, les indicateurs de performance et les tableaux de bord en conformité avec l'ISO 27004:2016 ;
- l'audit interne du SMSI ;
- l'examen de la gestion d'un SMSI ;
- la mise en œuvre d'un programme d'amélioration continue ;
- la préparation pour un audit de certification ISO 27001.
- préparation au passage de l'examen de certification ISO 27001 LI

CEH V13 : CERTIFIED ETHICAL HACKER

Devenir CEH v13, c'est s'assurer un avenir prometteur dans la cybersécurité. Les cyberattaques ne cessant d'évoluer, les entreprises recherchent désespérément des talents capables de protéger leurs systèmes. La certification CEH v13, reconnue mondialement, est votre passeport pour accéder à des postes à haute responsabilité et à des rémunérations attractives. Grâce à notre formation complète, vous maîtriserez les dernières techniques de hacking éthique. Vous apprendrez à identifier les vulnérabilités, à mener des tests de pénétration et à mettre en œuvre des stratégies de défense robustes. En intégrant l'intelligence artificielle (IA), cette formation vous prépare à relever les défis de la cybersécurité de demain.

5 jours

code : CEHV13

Objectifs

- Comprendre les fondamentaux de la sécurité informatique, les protocoles réseau, les systèmes d'exploitation, les bases de données, etc. ;
- Maîtriser les outils et les techniques de piratage éthique classique et pilotée par l'IA ;
- Mener des audits de sécurité en évaluant la sécurité des systèmes d'information et identifier les failles ;
- Réagir rapidement et efficacement en cas de compromission des systèmes ;
- Développer une pensée analytique pour identifier les risques potentiels et proposer des solutions adaptées ;
- Se préparer à l'examen CEH® v13 et obtenir le titre de Certified Ethical Hacker.

Public Cible

- Responsables sécurité des systèmes d'information (RSSI) ;
- Auditeurs internes et externes ;
- dministrateurs réseaux et systèmes ;
- Ingénieurs réseaux et systèmes ;
- Analystes en cybersécurité ;
- Toute personne souhaitant se spécialiser dans la sécurité informatique.

Prérequis

- Avoir 2 ans d'expérience minimum dans le domaine de la sécurité informatique.
- Savoir lire et comprendre l'anglais pour consulter les supports de cours, les labs et passer l'examen.

PROGRAMME

Module 1 : Introduction au hacking éthique
Module 2 : Techniques d'empreinte et de reconnaissance
Module 3 : Analyse des réseaux
Module 4 : Techniques d'énumération
Module 5 : Analyse des vulnérabilités
Module 6 : Hacking des systèmes
Module 7 : Menaces des logiciels malveillants
Module 8 : Sniffing ou reniflage de paquets
Module 9 : Ingénierie sociale
Module 10 : Attaques par déni de service
Module 11 : Détournement de session
Module 12 : Contournement des IDS, pare-feu et honeypots
Module 13 : Hacking des serveurs Web
Module 14 : Hacking des applications Web
Module 15 : Injections SQL
Module 16 : Piratage des réseaux sans fil
Module 17 : Hacking des appareils mobiles
Module 18 : Piratage IoT et OT
Module 19 : Sécurité du cloud computing
Module 20 : Cryptographie

COMPTIA SECURITY + : LES BASES DE LA CYBERSECURITÉ

Avec les attaques informatiques que subissent les organisations, la sécurité des infrastructures fait partie des points importants qui préoccupent tous les secteurs. En tant que professionnel de l'informatique, développer des compétences en cybersécurité devient indispensable pour démarrer ou poursuivre une carrière. De plus en plus d'entreprises proposent des postes d'administrateur sécurité ou encore d'auditeur informatique pour sécuriser leur système d'information, leur application et leur matériel. Notre formation CompTIA S+ vous permet d'acquérir des connaissances et des compétences pratiques en cybersécurité.

5 jours

code : COMPTIAS

Objectifs

- Etablir un modèle de menaces pour protéger les points d'accès réseau et les services informatiques d'une entreprise ;
- Administrer un système de détection d'intrusion (IDS) afin de détecter les attaques vers un réseau ou une infrastructure informatique ;
- Mettre en œuvre une sécurité réseau avec la création et la configuration d'un hôte Bastion ;
- Créer et configurer une liste de contrôle d'accès (ACL) ;
- Etablir des services de pare-feu avec des règles personnalisées en appliquant des filtres dynamiques de paquets et un filtrage de périphériques ;
- Identifier les ports réseau et les différents outils de piratage les plus utilisés par les hackers ;
- Réaliser un balayage de port et s'en servir judicieusement pour protéger un système d'information ;
- Surveiller et identifier des attaques et des vulnérabilités pour les affaiblir avant leurs déploiements dans un système d'information ;
- Assimiler la virtualisation sécurisée, le déploiement d'applications sécurisées et les concepts d'automatisation ;
- Caractériser, conseiller et appliquer les meilleures solutions de sécurité au sein d'une entreprise ;
- Connaître et comprendre les lois et les politiques de sécurité informatique ;
- Repérer, examiner et répondre aux événements et incidents de sécurité ;

Public Cible

- Administrateur système
- Ingénieur système
- Directeur des Systèmes d'Information (DSI)
- Chef de projet / Responsable de projet
- Technicien Support / HelpDesk
- Développeur
- Auditeur interne / externe

Prérequis

- Savoir lire et comprendre l'anglais, le japonais, le portugais ou l'espagnol pour le passage de l'examen SY0-701 ;
- Avoir obtenu la certification CompTIA Network+ et 2 ans d'expérience en tant qu'administrateur système ou sécurité (recommandé).

PROGRAMME

1. A propos de la cybersécurité
- Les notions de base de la sécurité informatique.
- La gestion des risques d'un projet informatique.
- L'évaluation de la vulnérabilité et du risque.

2. Comprendre les cyberattaques
- Le hacking et les hackers.
- La pratique de l'ingénierie sociale.
- Les programmes malveillants.
- Les attaques réseau.
- Les attaques de malwares.

3. Comprendre la cryptographie
- Les différentes techniques de cryptographie.
- Les infrastructures à clés publiques (ICP).

4. Connaitre les fondamentaux des réseaux
- Les composants de base d'un réseau.
- Le système d'adressage IP.
- Les ports réseaux et les ports logiciels.

5. Sécuriser un réseau d'entreprise
- Les composants de la protection réseau.
- Le chiffrement de la couche transport.
- L'amélioration des performances du réseau.
- L'analyse et la détection des anomalies.

6. Sécuriser des hôtes et assurer la confidentialité
- La sécurité des ordinateurs hôtes.
- La sécurité des données.
- La sécurité des appareils mobiles.

7. Sécuriser les services réseaux
- La sécurité d'une application.
- La sécurité des machines virtuelles.
- La sécurité des services dans le cloud.

8. Comprendre les processus d'authentification
- Les différents types de facteurs d'authentification.
- Les différents types de protocoles d'authentification.

9. Comprendre le contrôle d'accès des SI
- Les différentes techniques de contrôle d'accès.
- La gestion des comptes utilisateurs.

10. Gérer les risques
- Les lois, les normes et les politiques de sécurité informatique.
- La formation des utilisateurs.
- La sécurité physique et la sûreté des systèmes d'information.

11. Planifier la récupération après sinistre
- La reprise après sinistre.
- La haute disponibilité.
- La tolérance de pannes et la récupération.
- La réponse aux incidents.

LABS Informatiques pour la mise en pratique en fin de chaque partie.

SÉCURITÉ DE L'INFORMATION & CYBERSÉCURITÉ

(GOUVERNANCE, CONFORMITÉ & GESTION DES RISQUES INFORMATIQUES)

Code	Formation	Durée
CISM	CISM® : Certified Information Security Manager / **avec certification**	5 Jours
CISA	CISA : Certified Information Sytems Auditor / **avec certification**	5 Jours
CISSP	CISSP : Certified Information Systems Security Professional / **avec certification**	5 Jours
CRISC	CRISC: Certified in Risk and Information Systems Control **/ avec certification**	5 Jours
CGEIT	CGEIT® : Certified in Governance of Enterprise IT **/ avec certification**	5 Jours
COBITF	COBIT® 2019 Foundation **/ avec certification**	3 Jours
COBITDI	COBIT® Design & Implementation **/ avec certification**	3 Jours
ISO27001F	ISO/IEC 27001 Foundation **/ avec certification**	2 Jours:
ISO27001LI	ISO/IEC 27001 Lead Implementer **/ avec certification**	5 Jours
ISO27001LA	ISO/IEC 27001 Lead Auditor **/ avec certification**	5 Jours
ISO27002F	ISO/IEC 27002 Foundation **/ avec certification**	2 Jours
ISO27002LM	ISO/IEC 27002 Lead Manager **/ avec certification**	5 Jours
ISO27005RM	ISO/IEC 27005 Risk Manager **/ avec certification**	3 Jours
ISO27005EBIOS	ISO/IEC 27005 Avec EBIOS **/ avec certification**	5 Jours
ISO27005RESILIA	ISO/IEC 27005 Avec RESILIA **/ avec certification**	5 Jours
ISO27005LRM	ISO/IEC 27005 Lead Risk Manager **/ avec certification**	5 Jours
ISO27701F	ISO/IEC 27701 Foundation **/ avec certification**	2 Jours
ISO27701LA	ISO/IEC 27701 Lead Auditor **/ avec certification**	5 Jours
ISO27701LI	ISO/IEC 27701 Lead Implementer **/ avec certification**	5 Jours
ISO22301F	ISO/IEC 22301 Foundation **/ avec certification**	2 Jours

SÉCURITÉ DE L'INFORMATION & CYBERSÉCURITÉ

(GOUVERNANCE, CONFORMITÉ & GESTION DES RISQUES INFORMATIQUES)

Code	Formation	Durée
ISO22301LI	ISO/IEC 22301 Lead Implementer **/ avec certification**	5 Jours
ISO22301LA	ISO/IEC 22301 Lead Auditor **/ avec certification**	5 Jours
LCSM	Lead Cloud Security Manager **/ avec certification**	5 Jours
CCSP	Certified Cloud Security Professional	5 Jours
CDPSE	Certified Data Privacy Solutions Engineer	5 Jours
CDPO	Certified Data Protection Officer **/ avec certification**	5 Jours
CISO	Chief Information Security Officer **/ avec certification**	5 Jours
PCIDSS	Protection des données de cartes bancaires	3 Jours
SEC001	Sécurité SI avancée	5 Jours
SEC002	Audit, indicateurs & contrôle sécurité	3 Jours
SEC003	Gouvernance Cyber pour Comités de Direction	2 Jours

(ANALYSE, DÉTECTION & RÉPONSE AUX INCIDENTS)

CSA	Certified SOC Analyst	3 Jours
CTIA	Certified Threat Intelligence Analyst	3 Jours
CHFI	Hacking Forensic Investigator	5 Jours
LFOREX	Lead Forensics Examiner	5 Jours
ISO27035LIM	ISO/IEC 27035 Lead Incident Manager **/ avec certification**	5 Jours
SEC004	Détection d'intrusions	4 Jours
SEC005	Analyse forensic & réponse incidents	5 Jours
SEC006	Ransomware : compréhension de la menace	2 Jours

SÉCURITÉ DE L'INFORMATION & CYBERSÉCURITÉ

(PENTEST, ÉTHIQUE & OFFENSIVE SECURITY)

Code	Formation	Durée
CEHV13	Certified Ethical Hacker v13 **/ avec certification**	5 Jours
CLEH	Certified Lead Ethical Hacker **/ avec certification**	5 Jours
CND	Certified Network Defender	5 Jours
CPTP	Certified Pen Testing Professional **/ avec certification**	5 Jours
LPTP	Lead Pen Test Professional **/ avec certification**	5 Jours
C-PEN	CompTIA PenTest+ **/ avec certification**	5 Jours
SEC007	Fondamentaux du hacking	3 Jours
SEC008	Offensive Security Certified Professional	5 Jours
SEC009	Hacking systèmes embarqués	4 Jours
SEC010	Les tests d'intrusion dans le cadre d'une mission d'audit	4 Jours

(CYBERSÉCURITÉ (TECHNIQUE & ARCHITECTURES)

CC	Certified in Cybersecurity **/ avec certification**	2 Jours
ISO27032LCM	ISO 27032 Lead Cybersecurity Manager **/ avec certification**	5 Jours
CSCU	Certified Secure Computer User	2 Jours
C-CASP	CompTIA CASP+	5 Jours
C-CYSA	CompTIA CySA+	5 Jours
C-SECU	CompTIA Security+	5 Jours
SEC011	Sécuriser les infrastructures SI	3 Jours
SEC012	Sécurité avancée réseaux & systèmes	5 Jours

SÉCURITÉ DE L'INFORMATION & CYBERSÉCURITÉ

(CYBERSÉCURITÉ (TECHNIQUE & ARCHITECTURES)

Code	Formation	Durée
SEC013	Protection antivirus & malwares MS	3 Jours
SEC014	Sécuriser Linux/Unix	3 Jours
SEC015	Sécuriser environnements virtualisés	2 Jours
SEC016	Sécurité réseau avancée	3 Jours
SEC017	Cybercriminalité & cyberguerre	2 Jours

(CLOUD SECURITY)

AZ500	Azure Security Engineer	5 Jours
SC300	Microsoft Identity & Access	5 Jours
SC200	Analyse sécurité Microsoft	4 Jours
NSE7	Fortinet NSE7	3 Jours
NSE6	FortiMail NSE6	3 Jours
NSE4	FortiGate Administrator	5 Jours
CCNA	Cisco CCNA 200-301	5 Jours
SEC018	Palo Alto Firewall Essentials	5 Jours
SEC019	Cisco Firewall ASA – installation	2 Jours
SEC020	Cisco Firewall ASA – administration	4 Jours
SEC021	Sécuriser les infrastructures du Système d'Information	4 Jours

MANAGEMENT D'ENTREPRISE ET GESTION DES PROJETS

PMP® : PROJECT MANAGEMENT PROFESSIONAL

Le PMP, acronyme de Project Management Professional, est une certification prestigieuse attestant des compétences et de l'expérience d'un chef de projet, manager de projet ou responsable de projet. Délivrée par le Project Management Institute (PMI), elle a été créée sur la base du guide PMBOK (Project Management Body of Knowledge), un référentiel de bonnes pratiques en gestion de projet. Très recherchée par les entreprises, la certification PMP atteste d'un haut niveau de professionnalisme et de la maîtrise des outils et techniques nécessaires pour conduire avec succès des projets complexes

5 jours

code : PMP

Objectifs

- Cette formation vise à vous transmettre les connaissances et compétences qui vous permettront d'identifier les différents acteurs, de maitriser les différentes phases, de gérer les ressources et d'évaluer un projet peu importe la méthodologie utilisée. Elle vous permet également de préparer et réussir la certification PMP du PMI qui fait de vous un expert en management de projet.

Public Cible

- Chefs de projet expérimentés souhaitant obtenir la certification PMP® ;
- Professionnels impliqués dans la gestion de projet, souhaitant approfondir leurs connaissances et méthodes de gestion de projet ;
- Professionnels de la gestion de projet qui ont obtenu la certification PMP et qui souhaitent maintenir leur statut de certifié.

Prérequis

- Une expérience en gestion de projet (même informelle).
- Des connaissances de base en gestion de projet.

Prérequis pour passer l'examen PMP®

- Une expérience professionnelle en gestion de projet :
- Avec un diplôme universitaire (Bac +4 ou équivalent) : au moins 36 mois d'expérience en gestion de projet, avec au moins 36 mois de direction de projet (lead).
- Sans diplôme universitaire (Bac ou équivalent) : au moins 60 mois d'expérience en gestion de projet, avec au moins 36 mois de direction de projet (lead).
- À savoir : l'expérience en gestion de projet doit être cumulée de manière non chevauchante. Autrement dit, les périodes durant lesquelles vous avez travaillé simultanément sur plusieurs projets ne sont comptabilisées qu'une seule fois.

PROGRAMME

Jour 1 : compréhension de l'environnement commercial d'un projet

1. Les fondements
2. L'alignement stratégique
3. Les bénéfices et la valeur du projet
4. La culture organisationnelle et la gestion des changements
5. La gouvernance du projet
6. La conformité du projet

Jour 2 : démarrage et planification du projet (1/2)

Démarrage

1. L'identification des parties prenantes et la communication avec elles
2. La formation de l'équipe
3. La mise en place d'une compréhension commune

Planification

4. La planification des projets
5. Le périmètre du projet et le contenu du produit.

Jour 3 : planification du projet (1/2)

1. L'échéancier
2. Les ressources
3. Le budget
4. Les risques
5. La qualité
6. L'intégration des plans

Jour 4 : direction de l'équipe

1. Le développer de vos compétences en leadership
2. La création d'un environnement collaboratif au sein de l'équipe
3. L'automatisation de l'équipe
4. Les performances des membres de l'équipe
5. La communication et la collaboration avec les parties prenantes
6. La formation des membres de l'équipe et des parties prenantes
7. La gestion des conflits

Jour 5 : soutien des performances de l'équipe projet, clôture et révision pour l'examen

1. Le soutien des performances de l'équipe projet
2. La clôture du projet ou de la phase
3. révision pour l'examen PMP®

- Présentation du format de l'examen PMP (types de questions : situationnelles, basées sur des formules, etc.).
- Révision des points clés du PMBOK® Guide 7e édition et des domaines de performance.
- Exercices et simulations d'examen avec correction et explication des réponses.
- Conseils et stratégies pour réussir l'examen (gestion du temps, techniques de lecture des questions et gestion du stress).

COBIT® 2019 FOUNDATION

Le référentiel COBIT 2019 est la plus récente version du framework informatique développé par l'ISACA (Information System Audit and Control Association) qui est désormais largement utilisé dans le monde. En effet, il propose une approche des meilleures pratiques et de la gouvernance applicables à une entreprise IT. Il se concentre sur les principes de l'information et de la technologie comme vecteur de croissance pour les entreprises et les administrations, quelle que soit leur taille.

3 jours

code : COBITF

Objectifs

- Comprendre le fondement, les avantages et les principales raisons d'utiliser le framework COBIT pour la gouvernance informatique et technologique ;
- Faire la différence entre les principaux éléments du framework COBIT 2019 et celui de COBIT 5 ;
- Connaitre les changements apportés aux principes du système de gouvernance et à la mise à jour du programme de publication COBIT ;
- Identifier les nouveaux aspects d'un système de gouvernance :
- Maîtriser tous les objectifs de COBIT 2019 par rapport à sa version 5 ;
- Comparer la gestion de la performance selon COBIT au regard de la maturité et des capacités.
- Connaitre la corrélation entre les guides de conception COBIT et les guides de mise en œuvre ;
- Enumérer les principaux avantages d'une analyse de rentabilité COBIT ;
- Comprendre la cohérence de COBIT avec les autres frameworks, normes et bases de connaissances existantes ;
- Créer un système de gouvernance personnalisé avec COBIT 2019 ;
- Etre bien préparé pour passer l'examen COBIT2019 et obtenir la certification COBIT Foundation.

Public Cible

- Chef de projet / Responsable de projet
- Chef d'entreprise / Dirigeant
- Manager
- Administrateur système
- Ingénieur système
- Auditeur interne / externe

Prérequis

- Avoir une bonne expérience pratique dans le domaine de la gestion des systèmes d'information.
- Une maîtrise de l'anglais technique est fortement recommandée, car la documentation fournie est disponible uniquement en anglais (la formation est dispensée en français).

PROGRAMME

1. Introduction au framework COBIT 2019
- Qu'est-ce que la gouvernance informatique et ses avantages.
- Le lien entre les exigences des parties prenantes et la gouvernance.
- Les atouts du modèle COBIT.
- Le contexte, les avantages et les raisons clés de la mise en œuvre de COBIT 2019.
- Le mode de fonctionnement et l'architecture du système COBIT 2019.
- Les documentations et la boîte à outils disponibles.
- Les différences et les aspects communs entre COBIT et d'autres référentiels.

2. Compréhension des lignes directrices COBIT 2019
- Les 6 lignes directrices du système de gouvernance.
- Les 3 lignes directrices du cadre de gouvernance.

3. Présentation du système de gouvernance et de ses composants
- Les objectifs à atteindre en matière de gouvernance et de gestion.
- Les composants du système de gouvernance.
- Les secteurs et domaines concernés par la mise en œuvre du système de gouvernance.
- Les caractéristiques de conception de COBIT 2019.
- Les domaines d'intervention.
- Les 11 facteurs de mise en œuvre.
- La cascade d'objectifs.

4. Compréhension des objectifs de gouvernance et de gestion
- Le cœur du modèle de gouvernance et de gestion.
- Listing détaillé des objectifs et de leurs relations.

5. Gestion des performances de COBIT 2019
- Le concept et les principes de gestion de la performance.
- Les niveaux de performance et les niveaux de maturité.
- La gestion de la performance des processus.
- La gestion des autres composants du système de gouvernance.

6. Personnalisation du framework COBIT 2019
- Les impacts liés aux critères conceptuels.
- La conception et le développement d'un système de gestion adaptatif.

7. Définition du business case COBIT 2109
- Qu'est-ce qu'un business case (cas d'affaires) ?
- Les composantes du business case
- L'analyse de rentabilité.

8. Intégration de COBIT 2019 dans les services informatiques
- Les objectifs et les approches du guide de mise en œuvre.
- Le cycle de vie de son implémentation.
- La corrélation entre le guide de déploiement et le guide de conception.

9. Préparation à l'examen COBIT 2019
- Révision du programme de formation COBIT 2019.
- Astuces et recommandations pour l'examen officiel.

PRINCE 2 FOUNDATION + PRACTITIONER

Le référentiel COBIT 2019 est la plus récente version du framework informatique développé par l'ISACA (Information System Audit and Control Association) qui est désormais largement utilisé dans le monde. En effet, il propose une approche des meilleures pratiques et de la gouvernance applicables à une entreprise IT. Il se concentre sur les principes de l'information et de la technologie comme vecteur de croissance pour les entreprises et les administrations, quelle que soit leur taille.

3 jours

code : COBITF

Objectifs

- Comprendre le fondement, les avantages et les principales raisons d'utiliser le framework COBIT pour la gouvernance informatique et technologique ;
- Faire la différence entre les principaux éléments du framework COBIT 2019 et celui de COBIT 5 ;
- Connaitre les changements apportés aux principes du système de gouvernance et à la mise à jour du programme de publication COBIT ;
- Identifier les nouveaux aspects d'un système de gouvernance :
- Maîtriser tous les objectifs de COBIT 2019 par rapport à sa version 5 ;
- Comparer la gestion de la performance selon COBIT au regard de la maturité et des capacités.
- Connaitre la corrélation entre les guides de conception COBIT et les guides de mise en œuvre ;
- Enumérer les principaux avantages d'une analyse de rentabilité COBIT ;
- Comprendre la cohérence de COBIT avec les autres frameworks, normes et bases de connaissances existantes ;
- Créer un système de gouvernance personnalisé avec COBIT 2019 ;
- Etre bien préparé pour passer l'examen COBIT2019 et obtenir la certification COBIT Foundation.

Public Cible

- Chef de projet / Responsable de projet
- Chef d'entreprise / Dirigeant
- Manager
- Administrateur système
- Ingénieur système
- Auditeur interne / externe

Prérequis

- Avoir une bonne expérience pratique dans le domaine de la gestion des systèmes d'information.
- Une maîtrise de l'anglais technique est fortement recommandée, car la documentation fournie est disponible uniquement en anglais (la formation est dispensée en français).

PROGRAMME

1. Introduction au framework COBIT 2019

- Qu'est-ce que la gouvernance informatique et ses avantages.
- Le lien entre les exigences des parties prenantes et la gouvernance.
- Les atouts du modèle COBIT.
- Le contexte, les avantages et les raisons clés de la mise en œuvre de COBIT 2019.
- Le mode de fonctionnement et l'architecture du système COBIT 2019.
- Les documentations et la boîte à outils disponibles.
- Les différences et les aspects communs entre COBIT et d'autres référentiels.

2. Compréhension des lignes directrices COBIT 2019

- Les 6 lignes directrices du système de gouvernance.
- Les 3 lignes directrices du cadre de gouvernance.

3. Présentation du système de gouvernance et de ses composants

- Les objectifs à atteindre en matière de gouvernance et de gestion.
- Les composants du système de gouvernance.
- Les secteurs et domaines concernés par la mise en œuvre du système de gouvernance.
- Les caractéristiques de conception de COBIT 2019.
- Les domaines d'intervention.
- Les 11 facteurs de mise en œuvre.
- La cascade d'objectifs.

4. Compréhension des objectifs de gouvernance et de gestion

- Le cœur du modèle de gouvernance et de gestion.
- Listing détaillé des objectifs et de leurs relations.

5. Gestion des performances de COBIT 2019

- Le concept et les principes de gestion de la performance.
- Les niveaux de performance et les niveaux de maturité.
- La gestion de la performance des processus.
- La gestion des autres composants du système de gouvernance.

6. Personnalisation du framework COBIT 2019

- Les impacts liés aux critères conceptuels.
- La conception et le développement d'un système de gestion adaptatif.

7. Définition du business case COBIT 2109

- Qu'est-ce qu'un business case (cas d'affaires) ?
- Les composantes du business case
- L'analyse de rentabilité.

8. Intégration de COBIT 2019 dans les services informatiques

- Les objectifs et les approches du guide de mise en œuvre.
- Le cycle de vie de son implémentation.
- La corrélation entre le guide de déploiement et le guide de conception.

9. Préparation à l'examen COBIT 2019

- Révision du programme de formation COBIT 2019.
- Astuces et recommandations pour l'examen officiel.

PROFESSIONAL SCRUM MASTER™ (PSM I)

La formation Professional Scrum Master (PSM I) est une première étape à franchir pour toute personne qui souhaite exceller dans la gestion de projets agile. Elle permet de se familiariser avec les principes et les pratiques de Scrum et de se doter des compétences requises pour devenir un Scrum Master efficace.
À travers ce programme PSM 1 de 3 jours, vous acquerrez une compréhension de base du cadre Scrum, de ses rôles, de ses événements et de ses artefacts. De plus, vous apprendrez à appliquer les valeurs et les principes de Scrum afin d'optimiser le travail d'équipe, d'améliorer la productivité et de livrer des produits de haute qualité.

3 jours

code : PSMI

Objectifs

- Comprendre le concept et les principes fondamentaux du cadre Scrum (les rôles, les événements, les artefacts, les outils, etc.) et son approche empirique ;
- Comprendre les notions d'incertitude et de complexité dans la livraison de produits ;
- Comprendre la signification et l'importance des valeurs de Scrum ;
- Comprendre la signification et l'importance de l'incrément Definition Of Done (DOD) ;
- savoir utiliser le backlog produit pour planifier avec agilité ;
- Comprendre l'importance d'avoir une gestion autonome de son équipe, les compétences humaines requises ainsi que le rôle du Scrum Master ;
- Identifier le rôle de leadership du Scrum Master au sein de son équipe ;
- Savoir coordonner des actions dans le cadre d'une gestion de projet agile ;
- Acquérir les compétences, attitudes et postures nécessaires pour devenir Scrum Master ;
- être préparé pour le passage de l'examen officiel Professional Scrum Master™ I.

Public Cible

- Chef de projet / Responsable de projet
- Manager
- Développeur
- Toute personne impliquée dans le développement d'un projet, comme les chefs de projet, les consultants ou les responsables de projet ;
- Scrums masters, Coachs agile/scrum ou Consultants souhaitant se perfectionner ;

Prérequis

- Avoir lu le Scrum Guide™ ;
- Avoir des connaissances de base sur les principes agiles ou le développement itératif et incrémentiel ;
- Savoir lire et comprendre l'anglais pour pouvoir passer les examens et étudier la documentation officiel.

PROGRAMME

1. Comprendre l'agilité

- Pourquoi l'agilité ?
- Le manifeste pour le développement agile.
- Les champs d'application de l'agilité.

2. Comprendre Scrum à l'aide de son guide

- **Le concept de Scrum :** l'empirisme ; les 3 piliers ; les valeurs.
- **Les 3 artefacts :** le product backlog ; le sprint backlog ;l'incrément (DOD).
- **Les 5 événements :** le sprint ; le sprint planning ; le daily scrum ; le sprint review ; le sprint retrospective
- **Les 4 rôles :** l'équipe Scrum ; le product owner ; le scrum master ; les développeurs.

3. Comprendre le rôle du Scrum Master

- **Qu'est-ce qu'un scrum master ?**
  - les qualités et les compétences ;
  - les relations avec les parties prenantes ;
  - le cumul des mandats.
- **Les bonnes pratiques :**
  - la vélocité agile ;
  - le backlog produit et l'user story ;
  - le suivi et les indicateurs d'information ;
  - la rétrospective.
- **Le franchissement des obstacles :**
  - les facteurs de réussite ;
  - la collaboration avec les parties prenantes ;
  - les obstacles classiques.
- **Le servant leader et le coach agile :**
  - Qu'est qu'un servant leader ;
- **Qu'est qu'un coach agile ?**
  - la posture du scrum master ;
  - l'identification des problèmes ;
  - la cohésion de l'équipe et les valeurs ;
  - la prise de décision en équipe ;
  - la gestion des conflits au sein de l'équipe.

4. Comprendre la mise à l'échelle

- Les règles de base d'une mise à l'échelle.
- Le développement d'un produit avec plusieurs équipes.
- L'implémentation des référentiels : Scrum de Scrum ; Nexus ; SaFe.

5. Se préparer à l'examen Professional Scrum Master™ I

- Etude de cas sur le rôle du Scrum Master.
- Examen blanc en anglais avec correction (QCM de 80 questions durant 60 minutes).
- Conseils et astuces pour réussir l'examen officiel

MANAGEMENT D'ENTREPRISE ET GESTION DES PROJETS

(GESTION DE PROJET & MANAGEMENT)

Code	Formation	Durée
C-PROJECT	CompTIA Project+ : fondamentaux de la gestion de projet IT	5 Jours
GEP01	Gestion de projet informatique	4 Jours
GEP02	Manager les risques des projets informatiques	2 Jours
GEP03	Réussir ses projets informatiques	5 Jours
DEVOPS01	DevOps® Foundation	2 Jours
DEVOPS02	DevOps® Engineering Foundation	2 Jours
DEVOPS03	DevOps Leader®	2 Jours
ITIL01	ITIL™ 4 Foundation : les fondamentaux du référentiel ITIL	3 Jours
ITIL02	ITIL™ 4 Leader : Digital and IT Strategy	3 Jours
ITIL03	ITIL™ 4 Specialist : Create, Deliver and Support	3 Jours
ITIL04	ITIL™ 4 Specialist : Drive Stakeholder Value	3 Jours
ITIL05	ITIL™ 4 Specialist : High Velocity IT	3 Jours
ITIL06	ITIL™ 4 Strategist : Direct, Plan and Improve	3 Jours
ISO20000LA	ISO 20000 Lead Auditor	5 Jours
ISO20000LI	ISO 20000 Lead Implementer	5 Jours
PSMI	Professional Scrum Master™ I	3 Jours
PSMII	Professional Scrum Master™ II	3 Jours
PSK I	Professional Scrum With Kanban	2 Jours

MANAGEMENT D'ENTREPRISE ET GESTION DES PROJETS

(AGILITÉ, MÉTHODES HYBRIDES & PILOTAGE PAR RÉSULTATS)

Code	Formation	Durée
PMP	Project Management Professional / **avec certification**	5 Jours
CAPM	CAPM® – Certified Associate in PM	3 Jours
DASM	Disciplined Agile Scrum Master (DASM)™	2 Jours
DASSM	Disciplined Agile Senior Scrum Master (DASSM)™	2 Jours
GEP04	AgilePM® Foundation	3 Jours
GEP05	Gérer un projet avec agilité	2 Jours
GEP06	Gestion Axée sur les Résultats (GAR)	3 Jours
GEP07	Gérer des projets avec MS Project	4 Jours
ISO21502LPM	ISO 21502 Lead Project Manager	5 Jours
PRINCE2_01	PRINCE2® 7 Foundation	3 Jours
PRINCE2_02	PRINCE2® 7 Practitioner	2 Jours
PRINCE2_03	PRINCE2 Agile® Foundation	2 Jours
PRINCE2_04	PRINCE2 Agile® Practitioner	3 Jours
PRINCE2_05	PRINCE2 Foundation + Practitioner	5 Jours
PSPOI	Professional Scrum Product Owner™ I	2 Jours
PSPOII	Professional Scrum Product Owner™ II	2 Jours

MANAGEMENT D'ENTREPRISE ET GESTION DES PROJETS

(ENTREPRENEURIAT, STRATÉGIE & CROISSANCE BUSINESS)

Code	Formation	Durée
MC001	Passer de l'idée à l'entreprise formelle	4 Jours
MC002	Optimiser son organisation avec le Lean Management	5 Jours
MC003	Sortie de crise & performance	3 Jours
MC004	Stratégie marketing basée sur SEO	3 Jours
MC005	Développer l'activité commerciale via réseaux sociaux	3 Jours
MC006	Techniques avancées de Growth Hacking	3 Jours
	(EXCELLENCE OPÉRATIONNELLE & OPTIMISATION DES PROCESSUS)	
GEP08	PMO : Piloter les projets en entreprise	3 Jours
MC007	Théorie du Changement – Planification stratégique	2 Jours
LSSYB	Lean Six Sigma Yellow Belt	2 Jours
LSSGB	Lean Six Sigma Green Belt	5 Jours
LSSBB	Lean Six Sigma Black Belt	6 Jours
	(RESSOURCES HUMAINES, DÉVELOPPEMENT DES COMPÉTENCES & INGÉNIERIE DE FORMATION)	
MC019	Recruter & intégrer efficacement	3 Jours
MC020	Construire un référentiel de compétences	2 Jours
MC021	Piloter les recrutements & attirer les talents	3 Jours
MC022	Exploiter et analyser les données RH pour piloter la performance	3 Jours
MC023	Gestion de la performance RH	3 Jours
MC024	Ingénierie de la formation	3 Jours
MC025	Évaluer une formation	2 Jours
MC026	Formation de formateurs	3 Jours

MANAGEMENT D'ENTREPRISE ET GESTION DES PROJETS

(LEADERSHIP, MANAGEMENT & TRANSFORMATION MANAGÉRIALE)

Code	Formation	Durée
MC008	Gestion du stress au travail	2 Jours
MC009	Gestion du temps & priorités	2 Jours
MC010	Gestion des conflits et des crises en entreprise	3 Jours
MC011	Prise de parole en public	3 Jours
MC012	Développer ses capacités managériales	2 Jours
MC013	Manager les équipes avec agilité	3 Jours
MC014	Devenir Manager – prise de fonction	3 Jours
MC015	Renforcer sa posture de Manager-Leader	3 Jours
MC016	Conduite du changement – démarche et outils	3 Jours
MC017	Animer un atelier collaboratif	1 Jour
MC018	Télétravail & collaboration	2 Jours
(MARKETING, VENTE & STRATÉGIES DIGITALES)		
MC027	Marketing digital pour décideurs	3 Jours
MC028	Communication 360°	3 Jours
MC029	Marketing stratégique & mix	3 Jours
MC030	Gestion de marque & e-réputation	2 Jours
MC031	Techniques de vente & négociation Commerciale	3 Jours
MC032	Prospection téléphonique	2 Jours
MC033	Gestion éfficace de la relation client	3 Jours
MC034	Stratégie digitale & réseaux sociaux	3 Jours


STANDARDS
REGULATIONS

CIA® CERTIFIED INTERNAL AUDITOR

Le Certified Internal Auditor (CIA) est une certification internationale de référence en audit interne, proposée par l'Institute of Internal Auditors (IIA). Elle valide une expertise approfondie dans des domaines clés tels que la gestion des risques, le contrôle interne et la gouvernance. Cette certification atteste de compétences avancées pour évaluer et améliorer les processus organisationnels, renforcer la conformité et optimiser la performance. Reconnue mondialement, elle reflète un engagement envers l'excellence professionnelle, l'éthique et les normes internationales de l'audit interne.

(3+3+3) jours

code : CIA

Objectifs

- Évaluer et améliorer les processus organisationnels
- Renforcer la gestion des risques
- Assurer la conformité réglementaire
- Promouvoir la gouvernance d'entreprise
- Maintenir des normes éthiques élevées
- Améliorer les performances organisationnelles
- Réussir les 3 examens de certification du programme CIA

Public Cible

- Auditeur interne / externe
- Contrôleur de gestion
- Manager
- Directeur financier
- Toute personne exerçant une activité professionnelle dans le domaine de l'audit, du contrôle interne, de l'assurance qualité, de la gestion des risques et de la conformité ;
- Toute personne désireuse de se lancer dans le monde de l'audit interne tout en obtenant une certification reconnue.

Prérequis

- Avoir enregistré un compte et créé un profil sur le CCMS de l'IIA ;
- Avoir réalisé une auto-évaluation à partir du CCMS ;
- Avoir une licence active qui permet d'accéder au Kit CIA Learning System.

PROGRAMME

CIA® 1 : les concepts de base de l'audit interne

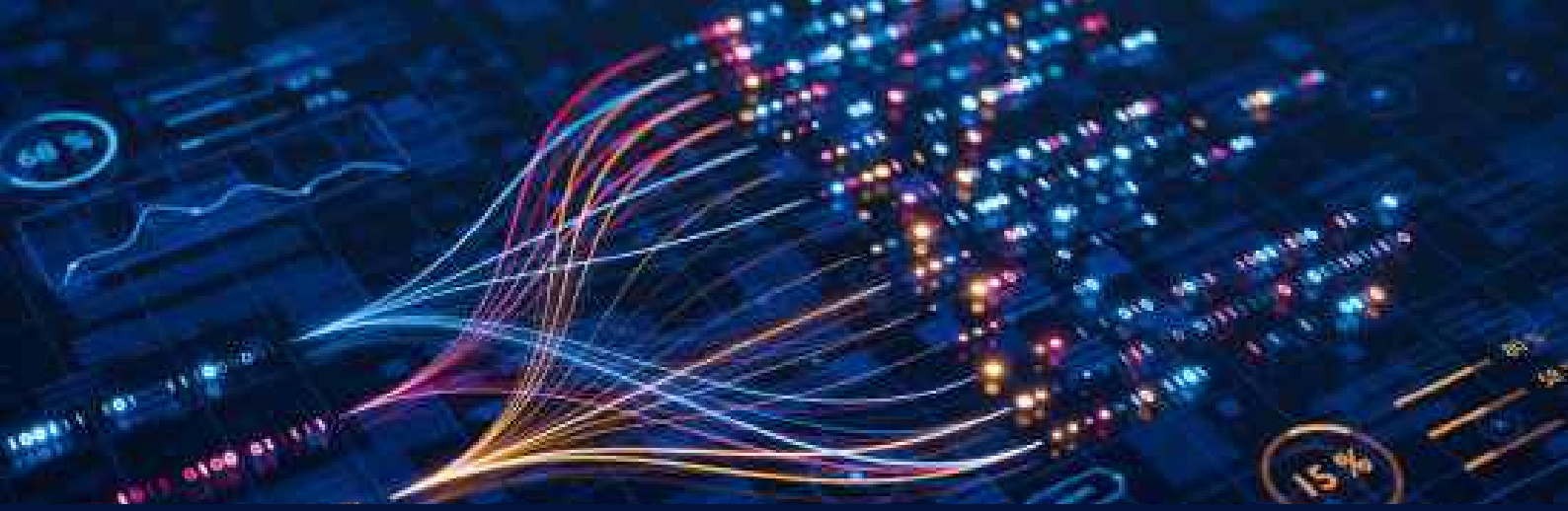
Domaine 1 : les principes fondamentaux de l'audit interne
Domaine 2 : l'indépendance et l'objectivité de l'auditeur interne
Domaine 3 : les compétences et la conscience professionnelle d'un auditeur interne
Domaine 4 : le programme d'assurance et d'amélioration qualité de l'audit interne
Domaine 5 : le modèle de maitrise de l'audit interne
Domaine 6 : la fonction de l'auditeur interne dans la prévention de la fraude

CIA® 2 : la pratique de l'audit interne

Domaine 1 : la gestion des activités d'audit interne
Domaine 2 : les étapes de planification d'une mission
Domaine 3 : les processus d'accomplissement de la mission
Domaine 4 : la communication des résultats de mission et le suivi

CIA® 3 : les connaissances commerciales pour l'audit interne

Domaine 1 : le sens des affaires
Domaine 2 : la sécurité de l'information
Domaine 3 : la technologie de l'information
Domaine 4 : la gestion financière



CISA® : CERTIFIED INFORMATION SYSTEMS AUDITOR

La certification CISA est un titre professionnel mondialement reconnu dans le domaine de l'audit, du contrôle et de la sécurité des systèmes d'information. Elle valide les compétences des auditeurs sur leur capacité à évaluer les vulnérabilités, à rédiger des rapports de conformité et à mettre en œuvre des contrôles au sein d'une entreprise.

5 jours

code : CISA

Objectifs

- Approfondir vos connaissances et améliorer vos compétences en audit des systèmes d'information ;
- Analyser et maîtriser les différents domaines sur lesquels porte l'examen du CISA ;
- Assimiler le vocabulaire et les idées directrices de l'examen CISA ;
- S'entraîner au déroulement de l'examen et acquérir les stratégies de réponse au questionnaire ;
- Se préparer et réussir l'examen officiel CISA®

Public Cible

- Auditeur interne / externe ;
- Auditeurs confirmés ;
- Informaticiens ou intervenants en audit des systèmes d'information qui souhaitent préparer l'examen et obtenir la certification CISA® délivrée par l'ISACA.

Prérequis

- Justifier d'au moins 5 ans d'expérience professionnelle à temps plein dans le domaine de l'audit, du contrôle, de l'assurance ou de la sécurité des Systèmes d'Information et des Technologies de l'Information (SI/TI). Cette expérience doit avoir été acquise dans les 10 années précédant la demande de certification.
- Avoir un niveau d'anglais technique permettant la compréhension de documents techniques (niveau B1/B2 du CECRL recommandé). La formation est dispensée en français.

PROGRAMME

Module 1 : compréhension d'un processus d'audit des SI
- Les standards de l'audit.
- L'analyse des risques ainsi que le contrôle interne.
- L'auto-évaluation.
- La réalisation d'un audit du Système d'Information.

Module 2 : compréhension de la gouvernance des TI
- La gouvernance.
- La stratégie de la gouvernance.
- Le Risk management.
- L'audit de la gouvernance.
- Les plans de continuité et de secours (SMCA).
- La réalisation d'un audit du SMCA.

Module 3 : acquisition, conception et implantation des SI
- Le cycle de vie des systèmes et de l'infrastructure.
- La pratique et l'audit d'un projet.
- Le développement.
- L'audit de la maintenance applicative et des systèmes.
- Les différents contrôles applicatifs.

Module 4 : exploitation, entretien et gestion des SI
- L'audit de l'exploitation des SI.
- L'audit des aspects matériels du SI.
- L'audit des architectures SI et réseaux.

Module 5 : protection des avoirs informatiques
- La gestion de la sécurité : politique et gouvernance.
- L'audit et la sécurité logique et physique.
- L'audit de la sécurité des réseaux.
- L'audit des dispositifs nomades.

Module 6 : préparation à l'examen CISA
- Présentation des types de questions de l'examen.
- Passage d'un examen blanc complet (correction détaillée et analyse des résultats).
- Conseils et stratégies pour réussir l'examen (gestion du temps, techniques de lecture des questions et gestion du stress).

ISO 31000 RISK MANAGER : MANAGEMENT DU RISQUE

Les entreprises sont confrontées à de multiples risques qui peuvent affecter sensiblement leurs performances économiques et leur image : considérations environnementales, questions de sécurité, problèmes sociétaux. Pour faire face à ces incertitudes au sein d'une organisation, il est important de mettre en place un management du risque selon les lignes directrices de l'ISO 31000.
Cette formation de manager vous donnera toutes les connaissances et compétences pour manager le risque à travers la compréhension et l'application de la norme ISO 31000:2018. Elle est parfaite pour vous permettre de maitriser les bonnes pratiques du management des risques afin de les implémenter dans une organisation et de poursuivre la mise en place de processus efficaces.

3 jours

code : ISO31000RM

Objectifs

- Maitriser tous les aspects de la gestion du risque selon la norme ISO 31000:2018 ;
- Mettre en place, maintenir et optimiser en continu un cadre de gestion du risque selon les directives de l'ISO 31000:2018 ;
- Intégrer le processus de gestion du risque selon les exigences de l'ISO 31000:2018.
- Réussir l'examen ISO 31000 Risk Manager et obtenir votre certification PECB Certified ISO 31000 Risk Manager.

Public Cible

- Manager
- Contrôleur de gestion
- Gestionnaire de personnel
- Chef d'équipe / Superviseur
- Chef de projet / Responsable de projet
- conseillers travaillant dans la gestion du risque.

Prérequis

- Avoir une bonne connaissance de base de la norme ISO 31000 ainsi que des notions avancées en management du risque.

PROGRAMME

Jour 1 : compréhension avancée des concepts et des principes de l'ISO 31000

- Présentation générale de la formation.
- La norme ISO 31000:2018.
- Le cadre organisationnel de management du risque.
- La mise en place d'un processus de management du risque.
- L'établissement du contexte de l'organisation.

Jour 2 : manager le risque selon la norme ISO 31000:2018

- L'identification des risques.
- L'analyse du risque.
- L'évaluation du risque.
- Le traitement du risque.
- L'acceptation du risque.
- La transmission d'information sur les risques.
- La surveillance et la révision du risque.

Jour 3 : mise en place des techniques d'appréciation du risque

- Les méthodologies de gestion du risque selon la norme ISO 31010:2019.
- préparation au passage de l'examen de certification ISO 31000 Risk Manager

CICS® CERTIFIED INTERNAL CONTROL SPECIALIST

Le contrôle interne, souvent considéré comme l'épine dorsale de la gestion d'entreprise, occupe une place centrale dans la réalisation des objectifs organisationnels et dans la réduction des risques. Il englobe un ensemble de pratiques, de politiques et de procédures visant à garantir l'intégrité, la fiabilité et la conformité des opérations d'une organisation.
Le programme de certification CICS a été développé par des professionnels du contrôle interne, leaders dans le domaine avec pour objectifs de valoriser et répandre la pratique et également de reconnaitre les compétences des talents en matière de contrôle interne. Ils ont pour but d'apporter de la valeur à la profession, aux professionnels du Contrôle Interne et aux employeurs.

5 jours

code : CICS

Objectifs

- Développer, mettre en place et gérer un système de contrôle interne au sein de votre organisation ;
- Déterminer les objectifs de votre organisation par rapport au contrôle interne ;
- Maîtriser les concepts, les pratiques et les principes fondamentaux du contrôle interne ;
- Renforcer la bonne gouvernance des processus et des activités ;
- Concevoir, déployer, gérer et évaluer un dispositif de contrôle interne ;
- Présenter l'épreuve d'obtention du CICS « Certified Internal Control Specialist ».

Public Cible

- Contrôleurs interne
- Auditeurs internes
- Directeurs financiers
- Comptables
- Gestionnaires de risques
- Professionnels de la conformité

Prérequis

- Avoir de l'expérience dans l'évaluation et la conception d'un système de controle interne.
- Avoir de l'expérience dans un métier de la conformité

PROGRAMME

Domaine 1 : Contrôle interne – Principes, termes et concepts

Domaine 2 : Environnement de contrôle interne

Domaine 3 : Gestion des risques

Domaine 4 : Évaluation des contrôles applicatifs

Domaine 5 : Évaluation des contrôles des systèmes de l'entreprise

Domaine 6 : Évaluation des risques

Domaine 7 : Mesure du contrôle interne et rapports

Domaine 8 : Pratiques de gouvernance

ISO 37301 LEAD IMPLEMENTER : MANAGEMENT DE LA CONFORMITÉ

Un système de management de la conformité ou Compliance Management System (CMS) conforme à la norme ISO 37301:2021 offre de multiples bénéfices. Il permet à une entreprise de minimiser ou de compenser les coûts, les risques et les préjudices causés par le non-respect des normes. De surcroît, il garantit la pérennité de l'entreprise et suscite la fiabilité, tout en encourageant les bonnes pratiques de gouvernance, la transparence et l'éthique dans les échanges commerciaux.

La **formation ISO 37301** destinée aux chefs conformité, responsables ou consultants, confère aux participants les connaissances requises pour créer, implémenter, gérer, maintenir et améliorer en continu un CMS.

5 jours

code : ISO37301LI

Objectifs

- Comprendre les concepts et les techniques nécessaires à la bonne exécution et à la bonne gouvernance d'un système de gestion de la conformité (CMS) ;
- Connaitre les synergies existantes entre la norme ISO 37301:2021 et d'autres normes ISO ;
- Appliquer des directives spécifiques de la norme ISO 37301:2021 dans un contexte propre à une entreprise.
- Accompagner une entreprise dans la planification, la mise en place, la gestion, la surveillance et la maintenance de son CMS ;
- Conseiller une entreprise sur les meilleures pratiques à adopter pour la gestion de la conformité ;
- Passer l'examen PECB Certified ISO 37301 Lead Implementer avec succès et obtenir une certification associée.

Public Cible

- Manager
- Chef de projet / Responsable de projet
- Chef d'entreprise / Dirigeant
- Chef d'équipe / Superviseur
- Ingénieur d'affaires
- Auditeur interne / externe

Prérequis

- Avoir des connaissances basiques sur les normes ISO standards applicables aux systèmes de gestion ;
- Avoir des connaissances basiques de la norme ISO 37301:2021 ou des directives de la norme ISO 19600 ;

PROGRAMME

Jour 1 : Introduction à ISO 37301 et initiation de la mise en œuvre d'un SMC

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts et principes fondamentaux du management de la conformité
- Initiation de la mise en œuvre d'un SMC
- Leadership et engagement
- Politique de conformité
- Rôles, responsabilités et autorité

Jour 2 : Mise en œuvre d'un SMC

- Contexte de l'organisation
- Périmètre du SMC
- Obligations de conformité
- Risques, opportunités et objectifs de conformité

Jour 3 : Mise en œuvre du SMC

- Ressources et compétences
- Sensibilisation et communication
- Gestion de l'information documentée
- Dispositifs de maîtrise
- Surveillance, mesure, analyse et évaluation

Jour 4 : Surveillance, amélioration continue et préparation à l'audit de certification du SMC

- Audit interne
- Revue de direction
- Non-conformité et actions correctives
- Amélioration continue
- Préparation à un audit de certification

Jour 5 : Préparation à l'examen de certification

GOUVERNANCE, AUDIT ET GESTION DES RISQUES

(GOUVERNANCE)

Code	Formation	Durée
CDTO	CDTO : Devenir responsable certifié de la transformation digitale	5 Jours
CGEIT	CGEIT : Professionnel certifié en gouvernance informatique d'entreprise	5 Jours
COBITF	COBIT2019 Foundation	3 Jours
COBITDI	COBIT Design & Implementer : Gouvernance et Audit SI	3 Jours
CISA	CISA : Certified Information Systems Auditor / **avec certification**	5 Jours
CRISC	CRISC : Certified in Risk and Informations Systems Control / **avec certification**	5 Jours
CRISC	CRISC : Certified in Risk and Informations Systems Control / **avec certification**	5 Jours
CISM	CISM : Certified Information Security Management / **avec certification**	5 Jours
TOGAF01	TOGAF® 9 Foundation : Compréhension du modèle d'architecture informatique d'entreprise	3 Jours
TOGAF02	TOGAF Practitioner **/ avec certification**	2 Jours
TOGAF03	TOGAF® 9 combined : maîtrise du modèle d'architecture informatique d'entreprise	5 Jours
ISO38500F	ISO/IEC 38500 Foundation : les fondamentaux de la gouvernance des TI	2 Jours
ISO38500CGM	ISO/IEC 38500 IT Corporate Governance Manager	5 Jours
ISO38500LCGM	ISO/IEC 38500 Lead IT : responsable principal de la gouvernance des TI	5 Jours
ISO27001LI	ISO 27001 Lead Implementer **/ avec certification**	5 Jours
ISO22301LI	ISO 22301 Lead Implementer **/ avec certification**	5 Jours
AGR001	Gouvernance informatique: les principaux réferentiels ITIL, COBIT, CMMI	5 Jours
AGR002	Plan de continuité d'activité SI (PCA/PRA)	5 Jours
AGR003	Reprise d'activité	5 Jours

GOUVERNANCE, AUDIT ET GESTION DES RISQUES

(AUDIT)

Code	Formation	Durée
AGR004	Conduite d'une mission d'audit interne (normes IIA)	4 Jours
AGR005	L'auditeur face à la fraude	3 Jours
AGR006	Audit interne : Mise en place & planning	4 Jours
CIA1	CIA® 1 – Concepts de base	3 Jours
CIA2	CIA® 2 – Pratique de l'audit interne	3 Jours
CIA3	CIA® 3 – Connaissances commerciales	3 Jours
AGR007	Fondamentaux de l' IT pour auditeurs	3 Jours
AGR008	Audit et révision des comptes : approche risque	2 Jours
AGR009	Pratique de l'audit interne dans les établissements bancaires	3 Jours
AGR010	Fondamentaux de l'audit interne	2 Jours
AGR011	Audit RH	2 Jours
AGR012	Audit des comptes du bilan	2 Jours
AGR013	Communication orale & écrite de l'auditeur	2 Jours
AGR014	Tests d'intrusion pour auditeurs	4 Jours

GOUVERNANCE, AUDIT ET GESTION DES RISQUES

(CONTRÔLE INTERNE & ET COMPLIANCE)

Code	Formation	Durée
CICS	Certified Internal Control Specialist	5 Jours
CFE	Certified Fraud Examiner	5 Jours
CICIP	Certified Internal Control Professional	5 Jours
CCM	Certified Compliance Manager	5 Jours
CAMS	Anti-Money Laundering Specialist	5 Jours
AMLMS	Anti Money Laundering Specialist	2 Jours
KYCY	Know Your Customer Specialist	2 Jours
SCS	Sanction Compliance Specialist	2 Jours
RCS	Regulatory Compliance Specialist	2 Jours
FATCACRSC	FATCA & CRS Specialist	2 Jours
AGR015	Contrôle de gestion : outils & méthodes	2 Jours
AGR016	Tableaux de bord & reporting	3 Jours
AGR017	Outils avancés de contrôle de gestion	3 Jours
AGR018	Les techniques de détection de la fraude et de réalisation des investigations	4 Jours

GOUVERNANCE, AUDIT ET GESTION DES RISQUES

(MANAGEMENT DES RISQUES & ANTICORRUPTION)

Code	Formation	Durée
ISO27005RM_01	ISO 27005 Risk Manager	3 Jours
ISO27005RM_02	ISO/CEI 27005 Lead Risk Manager	5 Jours
ISO31000F	ISO 31000 Foundation	2 Jours
ISO31000RM	ISO 31000 Risk Manager	3 Jours
ISO31000LRM	ISO 31000 Lead Risk Manager	5 Jours
MEHARI	Certified MEHARI Risk Manager	3 Jours
EBIOS	Certified EBIOS Risk Manager	3 Jours
ISO27005RM_03	ISO27005 Risk Manager + MEHARI	5 Jours
ISO27005RM_04	ISO27005E Risk Manager + EBIOS	5 Jours
COSO	COSO ERM Certificate	3 Jours
CRMA	Certified in Risk Management Assurance	3 Jours
AGRC19	AGRC06 – Cartographie des risques	2 Jours
AGRC20	AGRC07 – Mesure, maîtrise, surveillance des risques	2 Jours
AGRC21	Méthodes d'Identification & gestion des risques	3 Jours
AGRC22	AGRC19 – Méthodes d'appréciation des risques	5 Jours
ISO37001I	ISO 37001 Introduction	1 Jour
ISO37001F	ISO 37001 Foundation	2 Jours
ISO37001LI	ISO 37001 Lead Implementer	5 Jours
ISO37001LA	ISO 37001 Lead Auditor	5 Jours
ISO37001F	ISO37001F – Foundation certifié	2 Jours

GOUVERNANCE, AUDIT ET GESTION DES RISQUES

(MANAGEMENT DES RISQUES & ANTICORRUPTION)

Code	Formation	Durée
ISO37001LILI	ISO37001LI – Lead Implementer certifié	5 Jours
ISO37001LALA	ISO37001LA – Lead Auditor certifié	5 Jours
ISO37301F	ISO 37301 Foundation	2 Jours
ISO37301LI	ISO 37301 Lead Implementer	5 Jours
ISO37301LA	ISO 37301 Lead Auditor	5 Jours


Health
Quality of Environment
Financial Wellbeing
Social tionships
Quality of Life
Belong
Emotional Wellbeing
Work
Personal Safety

ISO 9001 LEAD IMPLEMENTER : MANAGEMENT DE LA QUALITÉ

Dans la famille des normes ISO 9000, la norme ISO 9001 est une des références dans le domaine du management de la qualité. Elle est destinée à toute entreprise, PME ou TPE, quel que soit son secteur d'activité. À ce jour, on compte 1 million d'entreprises et d'organismes certifiés ISO 9001 répartis à travers 170 pays.
Cette formation ISO 9001 Lead Implementer vous permettra d'acquérir les connaissances et les prérequis nécessaires pour guider une entreprise dans le déploiement d'une démarche qualité et plus spécifiquement dans la mise en place d'un SMQ conforme à la norme ISO 9001.

5 jours

code : ISO9001LI

Objectifs

- Comprendre la corrélation entre la norme ISO 9001 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMQ
- Savoir interpréter les exigences de la norme ISO 9001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMQ
- Aider une entreprise dans sa préparation à un audit de certification effectué par un organisme tierce.
- Réussir l'examen PECB ISO 9001 Lead Implementer et décrocher l'une des 4 certifications associées.

Public Cible

- 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

- Avoir des connaissances de base sur les normes des systèmes de management (ISO 9001:2015) et des principes de mise en œuvre des SMQ

PROGRAMME

Jour 1 : présentation de l'ISO 9001 et mise en œuvre du SMQ

- Revue des objectifs et du déroulement de la formation.
- Rappel sur les normes ISO, les systèmes de management et la famille ISO 9000.
- Introduction sur la qualité et les SMQ fondés sur ISO 9001.
- Introduction sur l'implémentation d'un SMQ.
- Compréhension du leadership et de l'engagement.
- La mise en place d'une politique qualité.
- Les rôles, les responsabilités et les niveaux d'autorité.

Jour 2 : planification du SMQ

- Le contexte de l'organisation
- Le champ d'application du SMQ
- Les mesures à prendre face aux risques et aux perspectives d'avenir.
- Les objectifs en matière de qualité
- La gestion du changement
- Les ressources et les compétences nécessaires.

Jour 3 : implémentation du SMQ

- La gestion des ressources.
- La prise de connaissance et la mise en place des actions de communication.
- La gestion de la documentation.
- Le contrôle opérationnel.
- Les spécifications du produit et sa conception.
- La mise en place d'un processus d'achat.
- La mise en production et la livraison du service.

Jour 4 et 5 : monitoring, mesure, amélioration continue et audit de certification

- Les outils de surveillance, de mesure, d'analyse et d'évaluation.
- L'audit interne.
- La revue de direction.
- Le traitement des éléments non-conformes.
- L'amélioration continue.
- La préparation à l'audit de certification ISO 9001LI
- Préparation au passage de l'examen PECB Certified ISO 9001 Lead Implementer : exercices de révision et QCM préparatoire

ISO 45001 LEAD IMPLEMENTER : SANTÉ ET SÉCURITÉ AU TRAVAIL

La norme ISO 45001 pose légitimement la question de faire évoluer tout collaborateur et toute personne extérieure dans un environnement sain et suffisamment protégé contre toute atteinte physique et psychologique.
Améliorer ses indicateurs comme les taux d'absentéisme, de turnover ou le nombre d'accident de travail voire de décès apportera une vraie plus-value au développement d'une société et instaurera un climat de confiance auprès de toutes les parties intéressées (collaborateurs, fournisseurs, clients, sous-traitants…).
La formation Lead Implementer vous permet d'adopter une méthodologie reconnue et développée par des professionnels internationaux, d'initier l'implémentation de la norme en mode projet, de définir les outils adéquats de contrôle et de surveillance et d'engager votre entreprise dans une démarche d'amélioration continue.

5 jours

code : ISO45001LI

Objectifs

- Réduire les accidents du travail, les maladies et les décès
- Fournir un environnement sécurisé pour exercer
- Améliorer le rendement et l'efficacité de la politique de la santé et de la sécurité au travail
- Protéger et améliorer la notoriété de la marque
- Economie en termes de coûts
- Transformer les opérations de détection en mode de prévention
- Améliorer le respect des législations en vigueur,
- réussir l'examen PECB ISO 9001 Lead Implementer et décrocher l'une des 4 certifications associées.

Public Cible

- Chef d'équipe / Superviseur
- Chef d'entreprise / Dirigeant
- Responsables ou consultants impliqués dans le management de la santé et de la sécurité au travail
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la santé et de la sécurité au travail
- Membres d'une équipe du SMSST

Prérequis

- Avoir une bonne connaissance de la norme ISO 45001 et des connaissances des principes de sa mise en œuvre.

PROGRAMME

Jour 1 : Introduction au concept de SMSST tel que défini par l'ISO 45001

- Introduction aux systèmes de management et à l'approche processus.
- Principes fondamentaux de la Santé et de la Sécurité au Travail.
- Présentation de la norme ISO 45001.

Jour 2 : Planifier la mise en œuvre d'un SMSST

- Définition du périmètre (domaine d'application).
- Développement de la politique et des objectifs de la Santé et de la Sécurité au Travail SMSST.
- Sélection de l'approche et de la méthode d'identification des risques d'évaluation des risques et contrôle des risques.

Jour 3 : Mettre en place un SMSST basé sur l'ISO 45001

- Mise en place d'une structure de gestion de la documentation.
- Conception des mesures de sécurité et rédaction des procédures.
- Implémentation des mesures de sécurité.
- Communication à propos de la Santé et de la Sécurité au Travail.
- Mise en œuvre des mesures de sécurité et processus de réponse.

Jour 4 et 5 : Contrôler, surveiller, mesurer et améliorer un SMSST

- Contrôler et surveiller un SMSST.
- Développement de métriques, d'indicateurs de performance et de tableaux de bord.
- Audit interne ISO 45001
- Revue de direction du SMSST.
- Mise en œuvre d'un programme d'amélioration continue.
- Préparation au passage de l'examen PECB Certified ISO 45001 Lead Implementer : exercices de révision et QCM préparatoire

ISO 14001 LEAD IMPLEMENTER : MANAGEMENT ENVIRONNEMENTAL

Ce cours intensif de 5 jours vous apportera une connaissance approfondie des meilleures pratiques mises en œuvre dans le cadre d'un Système de Management Environnemental (SME) conformément à la norme ISO 14001:2015.
Par cette approche systématique de management environnemental, votre organisation atteindra un équilibre entre l'environnement, la société et l'économie essentiels à une démarche de développement durable.
Cette formation vous permettra d'acquérir une expertise et un savoir-faire dans les domaines de la gestion de projets conformément aux lignes directrices de l'ISO 10006, des principes, systèmes et techniques de mise en œuvre d'un SME suivant l'ISO 14004, et des exigences pour les processus et équipements de mesure suivant l'ISO 10012.

5 jours

code : ISO14001LI

Objectifs

- Identifier et situer les enjeux environnementaux de l'entreprise
- Acquérir les connaissances nécessaires à la maîtrise des exigences de la norme ISO 14001 : 2015
- Exploiter efficacement le référentiel ISO14001
- Comprendre et savoir mettre en œuvre les méthodes et outils de la norme
- Acquérir des bases méthodologiques pour conduire une démarche de mise en place d'un SME
- Concevoir une documentation SME
- Passer l'examen de certification ISO 14001 Lead Implementer

Public Cible

- Responsable QSE
- Responsable ou coordinateur Environnement.
- Le responsable qualité
- Responsable du projet de certification ISO 14001 :2015.
- Auditeur ISO 14001.
- L'animateur HSE
- Chefs de Services Concernés

Prérequis

- Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre.

PROGRAMME

JOUR 1 : INTRODUCTION, COMPREHENTION DES EXIGENCES ISO 14001 – Version 2015

- Les principes de la norme
- Introduction aux concepts de mise en œuvre et gestion du management environnemental (SME)
- Les exigences légales et réglementaires spécifiques
- Les conditions de la réussite de la mise en place d'un SME
- Préparation au leadership

JOUR 2 : PLANIFICATION DE LA SME

- Prise en compte du contexte interne et des contextes externes
- Identifier les risques et opportunités
- Définir le périmètre de l'action
- Identifier les personnes intéressées

JOUR 3 : MISE EN ŒUVRE D'UN SME

- Construction de la Politique Environnementale et communication
- Mise en place de l'organisation opérationnelle
- Information, formation et sensibilisation aux personnes intéressées
- Définir le programme d'actions
- Mettre en place les bonnes pratiques sur le terrain

JOUR 4 & 5 : EVALUATION, AMELIORATION CONTINUE

- Mise en place des outils de contrôle de conformité et d'exigences
- Traitement des non-conformités
- Réalisation d'audit interne
- Pilotage d'actions correctives d'améliorations
- Management des revues de directions et communication avec les personnes intéressées
- Préparation au passage de l'examen PECB Certified ISO 14001 Lead Implementer : exercices de révision et QCM préparatoire

ISO 50001 LEAD IMPLEMENTER : MANAGEMENT DE L'ÉNERGIE

La norme ISO 50001 comporte un ensemble de lignes directrices pour inciter les entreprises et organisations à adopter un comportement responsable en matière de politique énergétique. Avec les enjeux climatiques et environnementaux d'aujourd'hui, appliquer un comportement énergétique responsable est primordial en termes d'image et de performance de l'organisation. Cette formation vous dispensera les compétences et les connaissances pour maîtriser le Système de management de l'énergie, depuis sa compréhension et son élaboration, jusqu'à sa mise en place et son suivi. Vous saurez ainsi comment manager une politique énergétique, de manière à réduire les consommations d'énergie et optimiser les performances de votre organisation.

5 jours

code : ISO50001LI

Objectifs

- Comprendre la corrélation entre la norme ISO 50001 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMÉ
- Savoir interpréter les exigences de la norme ISO 50001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMÉ
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de l'énergie

Public Cible

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

Prérequis

- Une bonne connaissance de la norme ISO 50001 et des connaissances approfondies des principes de mise en œuvre.

PROGRAMME

Jour 1 : Introduction à la norme ISO 50001 et au Système de Management de l'Energie (SME)

- Présentation générale de la formation
- La norme ISO 50001 et les autres règlements
- Le Système de management de l'énergie
- Les principes fondamentaux du SME
- Initialiser la mise en oeuvre du SME
- Comprendre l'organisme
- Analyser le système de management existant
- Leadership et approbation du projet

Jour 2 : Planifier le Système de management de l'énergie

- Définir le périmètre du SME
- Les politiques du SME
- Rôles, responsabilités et autorités
- Planifier et manager l'énergie

Jour 3 : Mettre en oeuvre le SME

- La responsabilité de la direction
- Les compétences, plan de formation et sensibilisation
- Plan de communication
- Gérer la documentation
- Concevoir des contrôles
- Rédiger des politiques et des procédures spécifiques
- Gérer les opérations
- Les processus d'achats

Jour 4 & 5 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SME

- Surveiller, mesurer, analyser et évaluer
- L'audit interne
- Revue de direction
- Traiter les non-conformités
- L'amélioration continue
- Préparer l'audit de certification
- Compétence et évaluation des implementers
- Préparartion à l'examen de certification ISO 50001 Lead Implementer

QUALITÉ, HYGIÈNE,SURETÉ ET ENVIRONNEMENT

(MANAGEMENT DE LA QUALITÉ)

Code	Formation	Durée
ISO9001F	ISO 9001 Foundation : Management de la qualité / **avec certification**	2 Jours
ISO9001LI	ISO 9001 Lead Implementer / **avec certification**	5 Jours
ISO9001LA	ISO 9001 Lead Auditor / **avec certification**	5 Jours
QHSE001	Implémentation et suivi de la démarche Qualité	3 Jours
QHSE002	Comprendre le Système de Management de la Qualité	3 Jours
QHSE003	Technique d'audit Qualité	3 Jours
QHSE004	Élaboration des documents du système qualité	3 Jours
QHSE005	Management par les processus	3 Jours
QHSE006	Initiation à la QHSE	2 Jours
QHSE007	Certification QHSE	2 Jours
QHSE008	Maîtrise statistique des procédés (MSP / SPC)	3 Jours
QHSE009	AMDEC produit / procédé / moyen	3 Jours
QHSE010	Analyse des non-conformités & plan d'actions	2 Jours
QHSE011	Audit interne de performance : méthodes avancées	3 Jours
QHSE012	Conception d'un SMQ digitalisé	2 Jours

QUALITÉ, HYGIÈNE,SURETÉ ET ENVIRONNEMENT

(SANTÉ & SÉCURITÉ AU TRAVAIL)

Code	Formation	Durée
ISO45001F	ISO 45001 Foundation	2 Jours
ISO45001LI	ISO 45001 Lead Implementer	5 Jours
ISO45001LA	ISO 45001 Lead Auditor	5 Jours
QHSE013	Les fondamentaux de la Santé & Sécurité au Travail	1 Jour
QHSE014	Equipier de Première Intervention / SST	1 Jour
QHSE015	Cadre réglementaire & prévention des risques professionnels	1 Jour
QHSE016	Identifier, analyser et évaluer les risques professionnels	3 Jours
QHSE017	Signalétique & signalisation de sécurité	2 Jours
QHSE018	Équipements de protection en SST	1 Jour
QHSE019	Risques de circulation interne	1 Jour
QHSE020	Plan de prévention & protocoles de sécurité	3 Jours
QHSE021	Sensibilisation à la sécurité au travail	3 Jours
QHSE022	Travail en hauteur	2 Jours
QHSE023	Être responsable HSE	2 Jours
QHSE024	Utilisation des extincteurs	3 Jours
QHSE025	Les dangers électriques	2 Jours
QHSE026	Port des EPI	2 Jours
QHSE027	Gestion des actions correctives	2 Jours
QHSE028	Espaces confinés	3 Jours
QHSE029	Améliorer la SST dans les PME	3 Jours

QUALITÉ, HYGIÈNE,SURETÉ ET ENVIRONNEMENT

(SANTÉ & SÉCURITÉ AU TRAVAIL)

Code	Formation	Durée
QHSE030	Fiche de prévention EPI	3 Jours
QHSE031	Inspection des échafaudages fixes	2 Jours
QHSE032	Santé & sécurité au travail dans les mines	2 Jours
QHSE033	Analyse des accidents (méthodes Arbre des causes / 5M)	2 Jours
QHSE034	Sécurité des machines (directive & normes CE)	3 Jours
QHSE035	Gestion de crise HSE	2 Jours
QHSE036	Psychologie du risque & culture sécurité	2 Jours
(PERFORMANCE & MÉTHODES D'AMÉLIORATION)		
LSSYB	Lean Six Sigma Yellow Belt	5 Jour
LSSGB	Lean Six Sigma Green Belt	4 Jours
LSSBB	Lean Six Sigma Black Belt	3 Jours
LSSGYB	Lean Six Sigma YB + GB	7 Jours
QHSE047	Méthodes & outils de résolution de problèmes	3 Jours
QHSE048	Kaizen – Amélioration continue	2 Jours
QHSE049	Pilotage des indicateurs de performance QHSE	2 Jours
QHSE050	Management visuel & animation des routines	2 Jours
QHSE051	Lean Office	2 Jours
QHSE052	Optimisez votre espace de travail avec la méthode 5S	3 Jours

QUALITÉ, HYGIÈNE,SURETÉ ET ENVIRONNEMENT

(ENVIRONNEMENT)

Code	Formation	Durée
ISO14001F	ISO 14001 Foundation	2 Jours
ISO14001LI	ISO 14001 Lead Implementer	5 Jours
ISO14001LA	ISO 14001 Lead Auditor	5 Jours
ISO50001F	ISO 50001 Foundation	2 Jours
ISO50001LI	ISO 50001 Lead Implementer	5 Jours
ISO50001LA	ISO 50001 Lead Auditor	5 Jours
ISO26000F	ISO 26000 Foundation	2 Jours
ISO26000LM	ISO 26000 Lead Manager	5 Jours
ISO26000LA	ISO 26000 Lead Auditor	5 Jours
QHSE037	Responsabilité Sociétale de l'Entreprise	2 Jours
QHSE038	Gestion des déchets	3 Jours
QHSE039	Prévention de la pollution & produits dangereux	2 Jours
QHSE040	Sensibilisation au développement durable	1 Jour
QHSE041	Gestion environnementale opérationnelle	3 Jours
QHSE042	Économie circulaire & stratégie durable	2 Jours
QHSE043	Analyse environnementale	2 Jours

QUALITÉ, HYGIÈNE,SURETÉ ET ENVIRONNEMENT

(SÉCURITÉ ALIMENTAIRE)

Code	Formation	Durée
ISO22001F	ISO 22001 Foundation	2 Jours
ISO22001LI	ISO 22001 Lead Implementer	5 Jours
ISO22001LA	ISO 22001 Lead Auditor	5 Jours
QHSE044	Méthode HACCP	2 Jours
QHSE045	Audit hygiène alimentaire & inspections internes	2 Jours
QHSE046	Hygiène en restauration collective et industrie	2 Jours

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

MICROSOFT CERTIFIED : POWER BI DATA ANALYST ASSOCIATE (PL-300)

Pour les entreprises, les administrations et les organisations, le métier d'analyste de données est un véritable atout. Sa première mission est de collecter et traiter les données afin de proposer des préconisations adaptées. Ses objectifs sont de donner vie aux données en les interprétant. En effet, il/elle extrait des informations issues de plusieurs flux dans le but de faciliter la prise de décision des managers. Pour ce faire, l'analyste de données utilise plusieurs outils, dont Power BI de Microsoft qui est une référence.
L'analyste de données Power BI travaille avec tous les acteurs clés d'une entreprise, quel que soit son secteur d'activité. Il identifie les besoins, trie et transforme les données, puis développe et crée des modèles de données avec Microsoft Power BI. Le data analyst Power BI crée de la valeur ajoutée grâce à des visualisations de données faciles à comprendre

5 jours **code : PL300**

Objectifs

- Connaître et décrire les possibilités et les fonctionnalités offertes par Microsoft Power Platform et ses produits associés ;
- Connaître et décrire les bénéfices commerciaux des différents produits de Power Platform ;
- Savoir comment fonctionne Microsoft Dataverse, les connecteurs et le AI builder ;
- Maîtriser le déploiement en mode multi-cloud avec Dynamics 365, Azure et d'autres applications connexes ;
- Créer et déployer des applications simples avec Power Apps, Power Automate, Power BI et Power Virtual Agents ;
- Collecter, filtrer et traiter des données ;
- Modéliser des données à des fins de performance et de scalabilité ;
- Elaborer et rédiger des rapports destinés à l'analyse de données ;
- Mettre en œuvre et exécuter des analyses approfondies sur les rapports ;
- Administrer et communiquer des données de rapport ;
- Réaliser des rapports paginés sous Power BI ;
- Réussir l'examen PL-300

Public Cible

- Administrateur système
- Chef de projet / Responsable de projet
- Contrôleur de gestion
- Comptable
- les professionnels Data ou de l'informatique décisionnelle désireux de se former à la pratique de l'analyse approfondie des données via Power BI ;

Prérequis

- Avoir une expérience professionnelle sur les données relationnelles et les données non relationnelles dans le Cloud

PROGRAMME

PL-900 : les fondamentaux de Microsoft Power Platform

Module 1 : découverte des composants de Power Platform
Module 2 : créer des solutions de données avec Dataverse
Module 3 : créer des applications d'entreprise avec Power Apps
Module 4 : automatiser les processus de travail avec Power Automate
Module 5 : analyser les données avec Power BI
Module 6 : créer des chatbots intelligents avec Power Virtual Agents
Labs informatiques :

L'analyse de données avec Microsoft Power BI PL-300

Module 1 : premiers pas avec Microsoft Data Analytics
Module 2 : créer des données sous Power BI Desktop
Module 3 : nettoyer, manipuler et insérer des données sous Power BI
Module 4 : créer un profil de données sous Power BI Desktop
Module 5 : créer des mesures dans Power BI Desktop via DAX
Module 6 : optimiser les performances d'un modèle de données
Module 7 : élaborer et optimiser des rapports de données
Module 8 : créer des tableaux de bord sous Power BI Desktop
Module 9 : créer des rapports paginés sous Power BI Desktop
Module 10 : effectuer une analyse approfondie
Module 11 : créer et organiser des espaces de travail
Module 12 : manager les jeux de données sous Power BI
Module 13 : sécuriser les données Power BI
Labs informatiques

AZURE DATABASE ADMINISTRATOR ASSOCIATE (DP-300)

Lorsqu'il s'agit de choisir un système de gestion de bases de données (SGBD), Microsoft Azure s'impose comme une solution incontournable. Azure SQL Database, un moteur de base de données PaaS (Platform as a Service), offre une gestion optimale des bases relationnelles en permettant aux administrateurs de se concentrer sur leurs activités principales d'administration et d'optimisation. Cette formation vous permettra d'acquérir les compétences théoriques et pratiques nécessaires pour devenir un administrateur associé de bases de données Azure certifié Microsoft.

5 jours **code : DP300**

Objectifs

- Enumérer les différents composants d'une base de données Azure ;
- Décrire les aspects d'une base de données relationnelle et non-relationnelle sur Azure ;
- Enumérer les différents modules d'un entrepôt de données (data warehouse) moderne dans Microsoft Azure ;
- Comprendre le fonctionnement d'une charge de traitement analytique dans Azure ;
- Préparer, installer et paramétrer les services de base de SQL Azure ;
- Préparer et gérer les ressources nécessaires au fonctionnement du SGBD ;
- Configurer un accès sécurisé pour les services Azure (identification, authentification, etc.) ;
- Monitorer et assurer l'optimisation des ressources de production ;
- Optimiser le traitement des requêtes SQL ;
- Réaliser une automatisation des tâches de travail ;
- Préparer et déployer un système de haute disponibilité et de reprise après incident ;
- Effectuer des opérations d'administration en utilisant le langage T-SQL ;
- Réussir l'examen DP-300 et obtenir la certification Azure Database Administrator Associate.

Public Cible

- Administrateur système
- Développeur
- Chef de projet / Responsable de projet
- Les professionnels informatique qui gèrent des données et des databases et qui désirent acquérir des connaissances sur l'administration des technologies de la plateforme de données Microsoft Azure

Prérequis

- Avoir une expérience professionnelle dans la gestion des bases de données et posséder des compétences techniques relatives aux solutions cloud ;
- Avoir administrer et développé avec SQL Server

PROGRAMME

Les fondamentaux de Microsoft Azure DP-900 (1 jour)

Module 1 : découverte et compréhension des fondements de donnée Azure
Module 2 : l'analyse des données relationnelles Azure
Module 3 : l'analyse des données non-relationnelles Azure
Module 4 : l'analyse moderne des entrepôts de données Azure
Labs informatiques

L'administration des bases de données relationnelles DP-300 (4 jours)

Module 1 : comprendre le rôle de l'administrateur associé de base de données Azure
Module 2 : planifier et gérer les ressources du SGBD Azure
Module 3 : créer un environnement Azure sécurisé et fiable
Module 4 : contrôler et optimiser les ressources de la structure de données
Module 5 : optimiser les performances des requêtes SQL
Module 6 : mettre en place des tâches automatisées
Module 7 : planifier et assurer la haute disponibilité ainsi que la reprise après sinistre
Labs informatiques

ISO 42001 LEAD IMPLEMENTER : MANAGEMENT DE L'INTELLIGENCE ARTIFICIELLE

Aujourd'hui, grâce aux progrès technologiques rapides, l'intelligence artificielle (IA) est presque partout. En effet, elle se généralise dans de nombreux domaines, mais son évolution nécessite des compétences spécifiques pour assurer sa bonne utilisation en respectant une éthique de qualité.
Cette formation vise à vous donner des compétences pratiques dans la mise en œuvre et la gestion responsable d'un système d'intelligence artificielle (SMIA) conformément à la norme ISO/IEC 42001 publiée en 2023.

5 jours **code : ISO42001LI**

Objectifs

- Comprendre le principe et le fonctionnement d'un système de management de l'intelligence artificielle basé sur la norme ISO/IEC 42001:2023 ;
- Connaitre les exigences spécifiques de l'ISO/IEC 42001 relative au responsable de mise en œuvre d'un SMIA ;
- Appliquer la méthode IMS2 du PECB et d'autres bonnes pratiques pour mettre en œuvre un SMIA conforme à l'ISO/CEI 42001 ;
- Accompagner une entreprise dans la mise en œuvre, la maintenance et l'amélioration continue d'un SMIA ;
- Accompagner une entreprise dans la préparation d'un audit de certification par un organisme indépendant ;
- réussir l'examen PECB ISO/IEC 42001 Lead Implementer.

Public Cible

- Chef de projet / Responsable de projet
- Manager
- tout professionnels chargés de superviser et de gérer des projets d'IA ;
- les consultants IA ;
- les conseillers experts et spécialistes cherchant à maîtriser la mise en œuvre pratique des SMIA conformément à l'ISO/IEC 42001 ;
- les membres des équipes impliqués dans la mise en œuvre de systèmes d'IA ;

Prérequis

- Avoir des connaissances de base sur la norme ISO 42001 et sur le fonctionnement d'un système de management de l'IA (SMIA)

PROGRAMME

Jour 1 : introduction à l'ISO/IEC 42001 et au SMIA

- Présentation de la norme ISO/IEC 42001:2023 et de son importance dans la gestion de l'intelligence artificielle (IA).
- Les principes fondamentaux d'un système de management de l'IA (SMIA).
- Les étapes initiales de la mise en œuvre d'un SMIA.
- L'identification des parties prenantes et des objectifs de la mise en œuvre.

Jour 2 : planification de la mise en œuvre d'un SMIA

- L'élaboration du plan de projet.
- L'identification des ressources nécessaires et l'attribution des responsabilités.
- Les indicateurs de performance clés (KPI) pour mesurer l'efficacité du SMIA.
- L'évaluation des risques potentiels liés à la mise en œuvre.
- La définition de stratégies d'atténuation.

Jour 3 : mise en œuvre d'un SMIA

- Le processus de mise en place des politiques et des procédures du SMIA.
- La formation du personnel sur les nouveaux processus et technologies liés à l'IA.
- L'intégration des outils de gestion de l'IA dans les processus opérationnels existants.
- L'évaluation de la conformité aux exigences de l'ISO/IEC 42001:2023.

Jour 4 : surveillance d'un SMIA, amélioration continue et préparation à l'audit de certification

- Les outils de surveillance et de contrôle des performances du SMIA.
- L'identification des opportunités d'amélioration continue.
- La préparation de l'audit de certification selon l'ISO/IEC 42001.
- La revue des exigences de conformité et des meilleures pratiques pour réussir l'audit.
- Préparation à l'examen de certification

CDMP : FONDAMENTAUX DU DATA MANAGEMENT

Aujourd'hui, grâce aux progrès technologiques rapides, l'intelligence artificielle (IA) est presque partout. En effet, elle se généralise dans de nombreux domaines, mais son évolution nécessite des compétences spécifiques pour assurer sa bonne utilisation en respectant une éthique de qualité.
Cette formation vise à vous donner des compétences pratiques dans la mise en œuvre et la gestion responsable d'un système d'intelligence artificielle (SMIA) conformément à la norme ISO/IEC 42001 publiée en 2023.

3 jours

code : CDMP

Objectifs

- Comprendre les principes de base du Data Management et de la gouvernance des données.
- Acquérir des compétences pratiques pour gérer efficacement les données.
- Apprendre les meilleures pratiques en matière de modélisation, qualité, sécurité, architecture.

Public Cible

- Managers
- Architectes
- Chefs de projet
- DSI
- Administrateurs de base de données
- Développeurs CDO
- Data Analyst / Data Quality Analyst, Data Architect.

Prérequis

- Compétences de base sur les SI et leurs architectures

PROGRAMME

Module 1 : Comprendre les Fondamentaux

- Introduction au Data Management et ses objectifs.
- Concepts clés : Données, Information et connaissance.
- Définitions et enjeux du Data Management.
- Entreprise orientée donnée : Avantages, Limites et Responsabilités.
- Compréhension approfondie du Big Data
- Présentation du Data Management Body of Knowledge (DMBOK).

Module 2 : Gestion Stratégique des Données

- Les données de référence en entreprise : Structures et Types.
- Identification et gestion des sources de données et métadonnées pertinentes.
- Cycle de vie de la donnée : Durée de vie, Viabilité et Modélisation.
- Exploration des différents types de bases de données.
- Mise en pratique à travers des études de cas concrets.

Module 3 : Gouvernance et Architecture des Données

- Compréhension de la Gouvernance des Données.
- Définition des rôles et responsabilités dans la gestion des données.
- Processus clés et architectures des référentiels.
- Étapes d'une démarche de gestion des données et exigences liées au Big Data.
- Mise en pratique à travers des études de cas concrets.

Module 4 : Intégration, Modélisation, Business Intelligence et Big Data

- Fusion des données : Principes fondamentaux, Histoire, Schémas et Solutions d'intégration.
- Structuration des données.
- Analyse des données stratégiques.
- Traitement des données massives : Historique, Concepts clés, Architectures et Solutions adaptées.
- Mise en pratique à travers des études de cas concrets.

Module 5 : Qualité et Sécurité des Données

- Enjeux de la Qualité des Données et du Data Quality Management.
- Critères d'évaluation de la qualité des données : Intégrité, Complétude, Cohérence.
- Stratégies et outils pour améliorer la qualité des données.
- Aspects juridiques, éthiques et sécuritaires liés à la gestion des données.
- Mise en pratique à travers des études de cas concrets.

FORTINET NSE 4 - FORTIGATE SECURITY ET FORTIGATE INFRASTRUCTURE

Avec des menaces informatiques de plus en plus sophistiquées et soutenues, les entreprises doivent intégrer des outils de sécurité complexes à déployer, à administrer et à maintenir. Fortinet®, l'un des leaders en matière de solutions de sécurité informatique propose un pare-feu nouvelle génération, FortiGate®. Il s'intègre au sein d'un seul et même système d'exploitation, le FortiOS®. C'est donc un ensemble de services qui permet d'avoir une gestion unifiée des menaces (UTM).
Notre **formation Fortinet Fortigate NSE4** qui dure 5 jours se compose en 2 parties. La première partie est consacrée à la sécurité. Elle vous permettra au cours des 2 premiers jours de prendre en main les principales fonctions de l'UTM de FortiGate®. Vous apprendrez à configurer le pare-feu, à configurer le service VPN avec les protocoles IPSEC, SSL et pour finir, à **lutter contre les malwares** et créer des filtres d'URL. Dans la seconde partie dédiée à l'infrastructure qui dure 3 jours, vous apprendrez à configurer le FortiGate® dans ses fonctions avancées (virtualisation, IPS, FSSO, DLP, etc.).

5 jours

code : NSE4

Objectifs

- dministrer Fortigate® en mode graphique GUI ou par ligne de commande CLI (génération de rapports, gestion des logs et diagnostics, analyse des tables de routage, inspection du trafic, déchiffrage de flux chiffré) ;
- neutraliser les différentes menaces issues de malwares ;
- mettre en place différents VPN de type SSL ou IPSEC ;
- authentifier les utilisateurs ;
- gérer l'antivirus ;
- configurer le proxy explicit ;
- déployer un cluster, faire du load balancing et comprendre l'accélération matérielle pour la haute disponibilité ;
- mettre en œuvre les Virtual Domain, les politiques antiDoS et le FSSO ;
- gérer le NAT et le routage ;
- implémenter l'IPv6 et le dual stack IPv4/IPv6 ;
- utiliser les Policy Based Routing(PBR) ;
- déployer des profils data leak prevention (DLP) ;
- être préparé pour le passage de l'examen FortiOS 7.0 Fortinet NSE4.

Public Cible

- Administrateur système
- Administrateur réseaux - télécoms
- Ingénieur système
- Tout professionnel de l'informatique qui doit administrer un firewall FortiGate® ou qui souhaite le découvrir ;
- Tout professionnel de la sécurité informatique qui désire passer la certification NSE 4 - FortiGate Network Security Professional.

Prérequis

- Une parfaite compréhension des couches du modèle OSI ;
- Une connaissance de base des protocoles Internet TCP/IP ;
- Une connaissance des concepts d'un firewall d'entreprise.

PROGRAMME

Partie 1 : Sécurité de Fortigate® (2 jours)

- Compréhension de Fortigate et de l'UTM.
- Gestion des logs et la supervision des équipements.
- Gestion des règles du firewall sans l'authentification des utilisateurs.
- Mise en œuvre d'un VPN SSL pour permettre l'accès distant au réseau de l'entreprise.
- Mise en œuvre d'un VPN IPSec.
- Gestion et le paramétrage de l'antivirus.
- Gestion de l'authentification des utilisateurs.
- Mise en œuvre d'un proxy explicit et la mise en cache.
- Gestion du contrôle applicatif.

Partie 2 : Infrastructure Fortigate® (3 jours)

- Analyse de la table de routage de Fortigate®.
- Mise en œuvre de la virtualisation.
- Mode transparent.
- Load balancing de trafic sur plusieurs opérateurs (haute disponibilité).
- Configuration avancée d'un VPN IPSec.
- Mise en œuvre de l'Intrusion Prevention Systems (IPS).
- Configuration du Single-Sign-On (FSSO).
- Déchiffrage des flux chiffrés.
- Déploiement des profils data leak prevention (DLP).
- Gestion des diagnostics.
- Fonctionnement de l'accélération matérielle.
- Paramétrage de l'IPv6.

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

(MANAGEMENT DES SERVICES INFORMATIQUES)

Code	Formation	Durée
ITIL01	ITIL™ 4 Foundation : les fondamentaux du référentiel ITIL	3 Jours
ITIL02	ITIL™ 4 Leader : Digital and IT Strategy	3 Jours
ITIL03	ITIL™ 4 Specialist : Create, Deliver and Support	3 Jours
ITIL04	ITIL™ 4 Specialist : Drive Stakeholder Value	3 Jours
ITIL05	ITIL™ 4 Specialist : High Velocity IT	3 Jours
ITIL06	ITIL™ 4 Strategist : Direct, Plan and Improve	3 Jours
ISO20000LI	ISO 20000 Lead Implementer	5 Jours
ISOI20000LA	ISO 20000 Lead Auditor	5 Jours
TIC001	IT Asset Management (Méthodes et bonnes pratiques)	3 Jours
TIC002	IT Operations Management	3 Jours
TIC003	Gestion de la capacité et de la disponibilité IT	2 Jours
TIC004	Service Desk Excellence : outils, KPI & performance	2 Jours

(CLOUD, INFRASTRUCTURE & DEVOPS)

AZ-305	Conception de solutions d'infrastructure Microsoft Azure	4 Jours
AZ-400	Conception et mise en œuvre DevOps	4 Jours
DP-201	Designing an Azure Data Solution	4 Jours
DEVP01	DevOps Engineer Expert	4 Jours
DEVP02	DevOps Foundation®	2 Jours
DEVP03	DevOps Leader®	2 Jours
TIC009	Docker & Kubernetes – Déploiement de conteneurs	4 Jours

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

(TRANSFORMATION DIGITALE)

Code	Formation	Durée
ISO42001F	ISO 42001 Foundation	2 Jours
ISO42001LA	ISO 42001 Lead Auditor	5 Jours
ISO42001LI	ISO 42001 Lead Implementer	5 Jours
AIRM	AI Risk Manager : gérer les risques liés à l'intelligence artificielle	5 Jours
CDTO	CDTO : devenir responsable certifié de la transformation digitale	5 Jours
TIC005	Artificial Intelligence Expert : maîtrise des techniques avancées	5 Jours
TIC006	Stratégie de transformation digitale : modèles & frameworks	2 Jours
TIC007	AI Essentials : IA générative pour les managers	2 Jours
TIC008	Product Owner & Product Management	3 Jours

(DATA, ANALYTICS & BUSINESS INTELLIGENCE)

PL-300	Microsoft Power BI Data Analyst Associate	5 Jours
PL-900	PL-900 : Fondamentaux Power Platform	2 Jours
TIC011	Data Architecture & Modeling	2 Jours
TIC012	Data Quality Management	2 Jours
TIC013	Explorer et comprendre les données	2 Jours
TIC014	Fondamentaux du Data Management (CDMP Associate)	4 Jours
TIC015	Python pour la Data (initiation)	3 Jours
TIC016	Modélisation de données (DAX & Power Query)	3 Jours
TIC017	Introduction au Big Data (Hadoop, Spark)	3 Jours
TIC018	Power BI – Initiation	3 Jours

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

(CERTIFICATIONS MICROSOFT AZURE / AWS)

Code	Formation	Durée
AI-102	Azure AI Engineer Associate	5 Jours
AI-900	Azure AI Fundamentals	1 Jour
AZ-303	Azure Architect Technologies	5 Jours
AZ-304	Azure Architect Design	4 Jours
DP-100	Azure Data Scientist Associate	5 Jours
DP-203	Azure Data Engineer Associate	5 Jours
DP-300	Azure Database Administrator Associate	5 Jours
DP-420	Azure Cosmos DB Developer Specialty	4 Jours
DP-900	Azure Data Fundamentals	1 Jour
AZ-204	Azure Developer Associate	5 Jours
AZ-305	Azure Solutions Architect Expert	4 Jours
AZ-900	Azure Fundamentals	3 Jours
TIC010	Les bases de Microsoft Azure	3 Jours

(MICROSOFT 365 & SERVICES CLOUD MICROSOFT)

MD-101	Managing Modern Desktops	5 Jours
MD-102	Microsoft Endpoint Administrator	5 Jours
MS-102	Microsoft 365 Enterprise Administrator Expert	5 Jours
MS-203	Messaging Administrator Associate	5 Jours
MS-900	Microsoft 365 – Les fondamentaux	1 Jour
SC-900	Microsoft SC-900 : Sécurité, conformité, identité	1 Jour

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

(MICROSOFT, CISCO, FORTINET, VEEAM & VMWARE)

Code	Formation	Durée
TIC019	Maitriser la configuration & gestion des switchs Cisco	4 Jours
TIC020	Programmer et automatiser des solutions Cisco	3 Jours
TIC021	Veeam Availability Suite v12 : configuration et gestion	3 Jours
TIC022	Veeam : conception avancée et optimisation	2 Jours
TIC023	VMware vSphere® 8 : installation, configuration et gestion	5 Jours
NSE4	Fortinet - FortiGate NSE 4 Fortigate Network Security Professional	5 Jours
NSE5	Fortinet - Administrer FortiAnalyser NSE5	3 Jours
NSE6	Fortinet - Fortiweb NSE 6	3 Jours
NSE7	Fortinet - FortiGate III NSE 7	3 Jours
	(BASES DE DONNÉES (ORACLE & MYSQL)	
TIC01	MySQL 5 : initiation & administration	4 Jours
TIC026	SQL Server Administration Niveau 1	4 Jours
TIC027	Optimisation des performances SQL	3 Jours
TIC028	PostgreSQL Administration	3 Jours
ORA01	Oracle Database 12c – Workshop Ed 1	5 Jours
ORA02	Oracle Database 12c – Security	5 Jours
ORA03	Oracle Database 19c – Optimisation	3 Jours
ORA04	Oracle Database 19c-21c – Administration	5 Jours

TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

(SYSTÈMES & LINUX / WINDOWS SERVER)

Code	Formation	Durée
TIC024	Administrateur Linux débutant (LPIC-1)	4 Jours
TIC025	Administration avancée Linux	4 Jours
AZ-800	Windows Server Hybrid Administrator Associate	5 Jours
MD-100	Modern Desktop Administrator Associate	5 Jours
	(DÉVELOPPEMENT LOGICIEL & PROGRAMMATION)	
ORA05	Programmation Java EE	5 Jours
ORA06	Programmation Java EE avancée	6 Jours
PL-400	Développeur Power Platform (PL-400)	5 Jours
PL-500	Développeur RPA Power Automate (PL-500)	4 Jours
0	Cisco Certified Network Professional (CCNP Enterprise)	5 Jours


ISO
CERTIFIED

ISO/IEC 27005 : RISK MANAGER

Cette formation vous fournira les connaissances essentielles et les compétences requises pour maîtriser toutes les étapes de la gestion des risques selon la méthode EBIOS. Ce que vous apprendrez : À travers des travaux pratiques, tels que des études de cas, Vous développerez une expertise qui vous permettra de réaliser une évaluation précise des risques liés à la sécurité de l'information. Vous apprendrez également à gérer le cycle de vie de ces risques.
Ce programme est également parfait pour ceux qui souhaitent implémenter la norme ISO/CEI 27001.

5 jours

code : ISO27005RM

Objectifs

- Maîtriser tous les principes, outils, méthodes et stratégies liés à la gestion des risques ;
- Être capable de gérer les informations sur les risques pour la sécurité conformément à la norme ISO 27001:2022 ;
- Avoir une bonne connaissance de la norme ISO/CEI 27005:2022 et de son application ;
- Développer des compétences pour mettre en œuvre, gérer et maintenir un programme de gestion des risques ;
- Comprendre les interrelations entre la gestion des risques en matière de sécurité de l'information, les contrôles de sécurité et la conformité aux obligations des différentes parties impliquées dans la logistique.

Public Cible

- Administrateur système
- Chef de projet / Responsable de projet
- Directeur des Systèmes d'Information (DSI)

Prérequis

- Une solide compréhension de la norme ISO/CEI 27005, ainsi que des techniques d'évaluation des risques associés à la sécurité de l'information.

PROGRAMME

Jour 1 : Gestion du risque selon la norme ISO 27005

- Introduction et concepts de base en gestion des risques, l'impact, la menace, la vulnérabilité.
- Présentation des normes et les cadres de référence ISO en gestion des risques : ISO 27001:2022 à ISO 27005:2022, ISO 31000:2018.
- Les lignes directrices pour les méthodologies d'analyse des risques.
- L'étude des objectifs de l'analyse avec les managers.
- L'approche quantitative et qualitative de l'évaluation des risques.

Jour 2 : Evaluation, traitement et gestion du risque selon ISO 27005

- La classification des actifs.
- L'identification, l'analyse et l'évaluation des risques.
- Les options de traitement du risque.
- Les plans de réduction par des mesures de sécurité.
- La gouvernance de la gestion des risques.
- Les principales méthodologies de gestion des risques: EBIOS, MEHARI, OCTAVE, CRAMM et Microsoft Security Compliance Management.

Jour 3 : Initier une analyse de risque avec EBIOS

- Introduction.
- Présentation de la notion de risques.
- Les 5 étapes de la méthode EBIOS.
- Application pratique de la méthode en petits groupes (2 à 3 personnes) sur un cas prédéfini :
- Les éléments essentiels.

Jour 4 et 5 : Application de la méthode EBIOS et conclusion d'une analyse de risques avec EBIOS

- La conduite d'une analyse des risques.
- Les expressions des besoins.
- Les vulnérabilités.
- Application pratique de la méthode en petits groupes (2 à 3 personnes) sur un cas prédéfini ;
- L'analyse des risques.
- Les objectifs de sécurité.
- Les couvertures des risques.

ISO 37001 LEAD IMPLEMENTER : SYSTÈME DE MANAGEMENT ANTI-CORRUPTION

Dans la famille des normes ISO, la norme ISO 37001 est une référence dans le domaine de la lutte contre la corruption. Elle s'adresse à toute organisation, quelle que soit sa taille ou son secteur d'activité. À ce jour, de nombreuses entreprises et organismes ont mis en place des systèmes de management anti-corruption conformes à la norme ISO 37001 à travers le monde. Cette formation ISO 37001 Lead Implementer vous permettra d'acquérir les connaissances et les compétences nécessaires pour guider une organisation dans la mise en œuvre d'un système de management anti-corruption (SMAC) conforme à la norme ISO 37001.

5 jours

code : ISO37001LI

Objectifs

- Comprendre la corrélation entre la norme ISO 37001 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMAC (Système de Management Anti-Corruption)
- Savoir interpréter les exigences de la norme ISO 37001 dans un contexte spécifique de l'organisation
- Conseiller un organisme sur les meilleures pratiques de lutte contre la corruption ;
- Aider une entreprise dans sa préparation à un audit de certification effectué par un organisme tiers pour ISO 37001
- Réussir l'examen PECB ISO 37001 Lead Implementer et décrocher l'une des certifications associées.

Public Cible

- Responsables ou consultants impliqués dans la lutte contre la 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 de l'ISO 37001
- Membres d'une équipe dédiée à la gestion anti-corruption

Prérequis

- Avoir une connaissance approfondie des principes de lutte contre la corruption ainsi qu'une familiarité avec les concepts de gestion d'actifs.

PROGRAMME

Jour 1 : Lancer le système de management anti-corruption

- La définition des objectifs anti-corruption alignés sur la stratégie.
- Les caractéristiques d'un Système de Management Anti-Corruption (SMAC).
- L'analyse de la norme ISO 37001:2025 et des enjeux de la corruption.
- L'initialisation du projet et la préparation de la mise en place.

Jour 2 : Planifier la mise en œuvre du SMAC

- L'élaboration de la politique anti-corruption et des rôles (Fonction de conformité).
- L'analyse du contexte et du système de management existant.
- La définition du périmètre du SMAC et la validation du projet.
- La conduite de l'appréciation des risques de corruption.

Jour 3 : Implémenter les contrôles et les opérations

- La gestion des procédures d'alerte (signalement) et de la communication.
- La mise en œuvre des contrôles opérationnels (financiers, non-financiers, cadeaux).
- La gestion des procédures et des informations documentées.
- La structuration de l'organisation et du management anti-corruption.

Jour 4 et 5 : surveiller, auditer et améliorer le système et préparer l'examen PECB ISO 37001 Lead Implementer

- Le pilotage de l'amélioration continue du SMAC..
- La conduite de l'audit interne et la revue de direction.
- Le traitement des non-conformités et la gestion des actions correctives.
- La surveillance, la mesure, l'analyse et l'évaluation de la performance.
- La préparation de l'audit de certification tierce partie.
- Présentation détaillée de l'examen (format étude de cas, questions rédactionnelles, domaines de compétences).
- Conseils et astuces pour réussir la certification (méthodologie de rédaction, gestion du temps, examen à livre ouvert).

ISO 22301 LEAD IMPLEMENTER : MANAGEMENT DE LA CONTINUITÉ D'ACTIVITÉ

Dans la famille des normes ISO, la norme ISO 22301 est une référence dans le domaine de la continuité des activités. Elle s'adresse à toute organisation, quelle que soit sa taille ou son secteur d'activité. À ce jour, de nombreuses entreprises et organismes ont mis en place des systèmes de management de la continuité des affaires conformes à la norme ISO 22301 à travers le monde. Cette formation ISO 22301 Lead Implementer vous permettra d'acquérir les connaissances et les compétences nécessaires pour guider une organisation dans la mise en œuvre d'un système de management de la continuité des affaires (SMCA) conforme à la norme ISO 22301.

5 jours

code : ISO22301LI

Objectifs

- Appliquer la norme ISO 22301:2019 au sein d'une organisation ;
- Maîtriser les concepts, pratiques et techniques pour implémenter et gérer un SMCA ;
- Accompagner l'organisation dans la planification, la mise en place, la gestion, la surveillance et la tenue à jour du SMCA ;
- Conseiller un organisme sur les meilleures pratiques relatives au SMCA. ;
- Réussir l'examen ISO 22301 Lead implementer et obtenir l'une des certifications « PECB Certified ISO 22301 Lead Implementer ;
- Mettre en œuvre la norme ISO 22301:2019 avec les autres règlements ;
-

Public Cible

- Responsables de la conformité d'un Système de Management de la Continuité d'Activité (SMCA)
- Personnes impliquées dans la gestion de la continuité d'activité (gestionnaires de risques, consultants, etc.)
- Tout membre d'une équipe SMCA
- Individus désireux de maîtriser l'implémentation d'un SMCA

Prérequis

- Etre impliqué dans la sécurité de système d'information et connaitre les principes fondamentaux de la norme ISO 22301 et de son application.

PROGRAMME

Jour 1 :

- Présentation générale de la formation.
- Introduction à la norme ISO 22301:2019.
- Principes et concepts du Système de Management de la Continuité d'Activité ;
- Compréhension de l'organisme, initialisation et mise en œuvre d'un SMCA.
- Analyse du système de management existant.
- Définition du périmètre du SMCA..

Jour 2 :

- Leadership et engagement.
- Politiques du SMCA.
- Structure organisationnelle.
- Information documentée.
- Compétences et Sensibilisation.
- Analyse de l'impact sur les activités.
- Appréciation du risque.

Jour 3 :

- Mesures de protection et d'atténuation.
- Procédures et plans de la continuité d'activité.
- Plan de réponse aux incidents.
- Plan d'intervention d'urgence.
- Plan de gestion de crise.
- Plan de reprise informatique.
- Plan de restauration.
- Plan de communication.

Jour 4 et 5 :

- Tests, exercices et mesure et surveillance du SMCA.
- Revue de direction et Audit interne.
- Traitement des non-conformités.
- Amélioration continue et préparation à l'audit de certification.
- Compétences et évaluation des implementers.
- Préparation au passage de l'examen de certification ISO 22301LI

NORMES ISO ET CONFORMITÉ

(TECHNOLOGIES NUMÉRIQUES)

Code	Formation	Durée
ISO27001F	ISO/IEC 27001 Foundation : management de la sécurité de l'information	2 Jours
ISO27001LI	ISO/IEC 27001 Lead Implementer : management de la sécurité de l'information	5 Jours
ISO27001AI	ISO/IEC 27001 Lead Auditor : management de la sécurité de l'Information	5 Jours
ISO27002F	ISO 27002 Foundation : code de bonne pratique pour le management de la sécurité de l'information	2 Jours
ISO27002LM	ISO 27002 Lead Manager : code de bonne pratique pour le management de la sécurité de l'information	5 Jours
ISO27005RM	ISO 27005 Risk Manager: gestion des risques liés à la sécurité de l'information	3 Jours
ISO27005EBIOS	ISO 27005 : certified Risk Manager avec EBIOS	5 Jours
ISO27005LRM	ISO 27005 Lead Risk Manager : gestion des risques liés à la sécurité de l'information	5 Jours
ISO27035LIM	ISO 27035 Lead Incident Manager : gestion des incidents de sécurité	5 Jours
ISO27032LCM	ISO 27032 Lead Cybersecurity Manager	5 Jours
CMMC	Certification du modèle de maturité en cybersécurité	5 Jours
ISO27701F	ISO/IEC 27701 Foundation : les fondamentaux d'un SMSI	2 Jours
ISO27701LI	ISO/IEC 27701 Lead Implementer : responsable de mise en œuvre d'un SMSI	5 Jours
ISO27701LA	ISO/IEC 27701 Lead Auditor : Responsable d'audit d'un SMSI	5 Jours
CLEH	Certified Lead Ethical Hacker : piratage éthique et tests d'intrusion	5 Jours
CDTO	CDTO : devenir responsable certifié de la transformation digitale	5 Jours
GDPRF	GDPR Foundation : les fondamentaux du Règlement Général sur la Protection des Données	2 Jours
CDPO	Certified Data Protection Officer	5 Jours
ISO42001F	ISO/IEC 42001 Foundation : les fondamentaux d'un SMIA	2 Jours
ISO42001LI	ISO/IEC 42001 Lead Implementer : responsable de mise en œuvre d'un SMIA	5 Jours

NORMES ISO ET CONFORMITÉ

(TECHNOLOGIES NUMÉRIQUES)

Code	Formation	Durée
ISO42001LA	ISO/IEC 42001 Lead Auditor : responsable auditeur d'un SMIA	5 Jours
ISO20000F	ISO/IEC 20000 Foundation : management de services des technologies de l'information	2 Jours
ISO20000LI	ISO/IEC 20000 Lead Implementer : management de services des technologies de l'information	5 Jours
ISO20000LA	ISO/IEC 20000 Lead Auditor : management de services des technologies de l'information	5 Jours
DRM	Disaster Recovery Manager : reprise d'activité des technologies de l'information	5 Jours
LDRM	Lead Disaster Recovery Manager : reprise d'activité des technologies de l'information	5 Jours
LPTP	Lead Pen Test Professional : expert en test d'intrusion	5 Jours
CLCM	Certified Lead Crisis Manager : devenir gestionnaire de crise certifié	5 Jours

(GOUVERNANCE, RISQUES & CONFORMITÉ)

ISO21502LPM	ISO 21502 Lead Project Manager : management de projet	5 Jours
ISO22301F	ISO 22301 Foundation : Management de la continuité d'activités	2 Jours
ISO22301LI	ISO 22301 Lead Implementer : Management de la continuité d'activités	5 Jours
ISO22301LA	ISO 22301 Lead Auditor : Management de la continuité d'activités	5 Jours
ISO38500F	ISO/IEC 38500 Foundation : les fondamentaux de la gouvernance des TI	2 Jours
ISO38500ICGM	ISO/IEC 38500 IT Corporate Governance Manager : responsable de la gouvernance des TI	3 Jours
ISO38500ILCGM	ISO/IEC 38500 Lead IT Corporate Governance Manager : responsable principal de la gouvernance des TI	5 Jours
ISO31000F	ISO 31000 Foundation : management du risque	2 Jours
ISO31000RM	ISO 31000 Risk Manager : management du risque	3 Jours
ISO31000LRM	ISO 31000 Lead Risk Manager : management du risque	5 Jours
ISO37001IN	ISO 37001 Introduction : système de management anti-corruption	1 Jour

NORMES ISO ET CONFORMITÉ

(GOUVERNANCE, RISQUES & CONFORMITÉ)

Code	Formation	Durée
ISO37001F	ISO 37001 Foundation : système de management anti–corruption	2 Jours
ISO37001LI	ISO 37001 Lead Implementer : système de management anti–corruption	5 Jours
ISO37001LA	ISO 37001 Lead Auditor : système de management anti–corruption	5 Jours
ISO37301F	ISO 37301 Foundation : les fondamentaux d'un CMS	2 Jours
ISO37301LI	ISO 37301 Lead Implementer : management de la conformité	5 Jours
ISO37301LA	ISO 37301 Lead Auditor : responsable d'audit d'un CMS	5 Jours
ISO55001F	ISO 55001 Foundation : management des actifs	2 Jours
ISO55001LI	ISO 55001 Lead Implementer : management des actifs	5 Jours
ISO55001LA	ISO 55001 Lead Auditor : management des actifs	5 Jours

(QUALITÉ, SANTÉ & SÉCURITÉ AU TRAVAIL)

ISO9001F	ISO 9001 Foundation : management de la qualité	2 Jours
ISO9001LI	ISO 9001 Lead Implementer : management de la qualité	5 Jours
ISO9001LA	ISO 9001 Lead Auditor : management de la qualité	5 Jours
ISO45001ISOF	ISO 45001 Foundation	2 Jours
ISO45001LI	ISO 45001 Lead Implementer : santé et sécurité au travail	5 Jours
ISO45001LA	ISO 45001 Lead Auditor : santé et sécurité au travail	5 Jours
ISO14001F	ISO 14001 Foundation : management environnemental	2 Jours
ISO14001LI	ISO 14001 Lead Implementer : management environnemental	5 Jours
ISO14001LA	ISO 14001 Lead Auditor : management environnemental	5 Jours
ISO50001F	ISO 50001 Foundation : management de l'énergie	2 Jours

NORMES ISO ET CONFORMITÉ

(QUALITÉ, SANTÉ & SÉCURITÉ AU TRAVAIL)

Code	Formation	Durée
ISO50001LI	ISO 50001 Lead Implementer : management de l'énergie	5 Jours
ISO50001LA	ISO 50001 Lead Auditor : management de l'énergie	5 Jours
ISO20121F	ISO 20121 Foundation : activité événementielle responsable	2 Jours
ISO20121LI	ISO 20121 Lead Implementer : activité evénementielle responsable	5 Jours
ISO20121LA	ISO 20121 Lead Auditor : activité evénementielle responsable	5 Jours
ISO26000F	ISO 26000 Foundation : responsabilité sociétale	2 Jours
ISO26000LM	ISO 26000 Lead Manager : maîtriser le management de la RSE	5 Jours
ISO22000F	ISO 22000 Foundation	2 Jours
ISO22000LI	ISO 22000 Lead Implementer	5 Jours
ISO22000LA	ISO 22000 Lead Auditor	5 Jours
ISO17025F	ISO/IEC 17025 Foundation : management de la qualité des laboratoires d'étalonnages et d'essais	2 Jours
ISO17025LI	ISO/IEC 17025 Lead Implementer : management de la qualité des laboratoires d'étalonnages et d'essais	5 Jours
ISO17025LA	ISO/IEC 17025 Lead Assessor : management de la qualité des laboratoires d'étalonnages et d'essais	5 Jours
ISO13485F	ISO 13485 Foundation : gestion de la qualité des dispositifs médicaux	2 Jours
ISO13485LI	ISO 13485 Lead Implementer : gestion de la qualité des dispositifs médicaux	5 Jours
ISO13485LA	ISO 13485 Lead Auditor : gestion de la qualité des dispositifs médicaux	5 Jours

ILS NOUS FONT CONFIANCE

SECURED SYSTEMS
INTERNATIONAL
MAKE YOUR BUSINESS SAFE

ABIDJAN, COCODY LES 2 Plateaux
Rue des OSCARS
18 BP M440 ABIDJAN 18
+225 2722280668 / 0798419519
contact@securedsys.net
www.securedsys.net

Bureaux internationaux

BUREAU DE PARIS
23 Rue Hélène, 78260 Achères
+33 631 664 974

BUREAU DE MONTREAL
1338 Rue des Calèches G3K0M8, Québec
+1 418 264 5120