CERTI TRUST
CONFIDENCE IN THE DIGITAL ERA



CATALOGUE DE FORMATIONS

Formation & Certification de Personnes



SOMMAIRE

Sécurité de l'information & Cybersécurité

- ISO 27001 Foundation 09
- ISO 27001 Lead Implementer 10
- ISO 27001 Lead Auditor 11
- ISO 27005 Risk Manager 12
- EBIOS Risk Manager 13
- Cybersecurity Foundation 14
- Cybersecurity Lead Implementer 15
- Cloud Security Foundation 16
- Rôle du RSSI 17
- HDS Foundation 18

Intelligence Artificielle & gouvernance IA

- Certified Ai Professional (CAIP) ISO/IEC 42001 Lead Implementer 20
- ISO/IEC 42001 Lead Auditor 21

Protection des données personnelles & Vie privée

- RGPD 23
- DPO 24
- LOI 09-08 25
- ISO 27701 Foundation 26
- ISO 27701 Lead Implementer 27

-

- ISO 22301 Foundation 29
- ISO 22301 Lead Implementer 30
- ISO 22301 Lead Auditor 31

Qualité, santé, sécurité

- ISO 9001 Foundation 33
- ISO 9001 Lead Auditor 34
- ISO 9001 Lead Implementer 35
- ISO 19011 Auditeur interne 36
- ISO 45001 Foundation 37
- ISO 45001 Lead Implementer 38
- ISO 45001 Lead Auditor 39

Environnement, ESG, Développement durable

- ISO 14001 Foundation 41
- ISO 14001 Lead Auditor 42
- ISO 14001 Lead Implementer 43
- ISO 26000 Foundation 44
- ISO 26000 Lead Implementer 45
- ISO 50001 Foundation 46
- ISO 50001 Lead Implementer 47
- Certified Energy Manager 48
- CBAM (Carbon Border Adjustment Mechanism mécanisme d'ajustement carbone aux frontières) 49
- ESG Manager- ISO 26000, CSRD & Climat 50

Risque, conformité & Anti-corruption

- ISO 31000 Foundation 52
- ISO 31000 Risk Manager certifié 53
- ISO 27005 Risk Manager (également lié à la sécurité) 54
- EBIOS Risk Manager (également lié à la sécurité) 55
- ISO 37001 Foundation 56
- ISO 37001 Lead Auditor 57
- ISO 37301 Foundation 58

Qui Sommes-Nous ?

CERTI-TRUST est une marque de services de certification regroupant plusieurs compagnies agissant de manière indépendante qui certifient les professionnels et réalisent des , des services de certification de personnes, de produits et de services dans le domaine des technologies de l'information et de la communication.
Afin de rendre plus accessibles les services de formation et de certification de personnes, **CERTI-TRUST** a développé une plateforme de formation et de certification en ligne facilement utilisable, innovante et permettant aux apprenants d'expérimenter leurs apprentissages de façon unique et enrichissante tout en bénéficiant d'une forte valeur ajoutée et d'un panier diversifié de contenus certifiants, le tout encadré par des formateurs compétents et très spécialisés dans l'ensemble des domaines enseignés.

Vision

Devenir un leader mondial des tests logiciels, de l'inspection et de la certification des systèmes de management, des professionnels et des produits.

Mission

Participer à la réussite des entreprises présentant une dépendance forte aux technologies de l'information en devenant leur tiers de confiance.

Valeurs

Compétence
Responsabilité
Transparence
Confidentialité
Réactivité.

Les certifications de personnes de Certi-Trust sont la preuve d'une conformité rigoureuse aux normes et à leurs conditions de mise en œuvre, reflétant ainsi la sécurité, la fiabilité et la haute qualité que nous apportons à nos produits de certification des compétences dans les différents domaines que nous couvrons.
Obtenir et conserver une certification Certi-Trust, c'est démontrer que l'on dispose des capacités nécessaires pour fournir les services professionnels attendus par la plupart des organisations qui sont engagées dans des démarches de mise en conformité ou de gestion maîtrisée de la sécurité, de la continuité d'activité, de la gestion des risques, de la Cybersécurité ou de tout autre système organisationnel ou technique.
Choisir d'être certifié et maintenir ses certifications c'est, pour chaque professionnel, assurer sur le long terme la mise en œuvre correcte et le support continu des systèmes de management et le respect des meilleures pratiques, des directives industrielles ou d'autres réglementations qui peuvent contribuer à aider les organisations à bénéficier des meilleures standards technologiques nationaux et internationaux.

ÉDITORIAL

Les formations en classe physique ne sont de nos jours plus totalement adaptées aux besoins de tous les participants en activité. Elles n'offrent pas la flexibilité et exigent de suivre toutes les parties de la formation au même rythme et dans une salle de formation. Pour les centaines de milliers de professionnels qui passent des formations certifiantes annuellement dans le monde, l'offre habituelle est ainsi monolithique, statique, descendante et inflexible, ne favorisant paradoxalement pas un véritable apprentissage. Suite à la crise sanitaire et le confinement qui s'en est suivi, les entreprises et leurs collaborateurs n'ont pas toujours pu trouver de solutions de rechange appropriées pour assurer les besoins en formation au sein de leurs organisations. Le potentiel de l'éducation à distance est ainsi aujourd'hui encore plus fort qu'il ne l'était précédemment mais la plupart des formations en ligne proposées aujourd'hui ne répondent pas adéquatement aux nouveaux besoins du moment. Elles sont réalisées en utilisant des outils de visioconférence avec partage de slides. Les participants sont obligés de rester plusieurs heures par jour devant un ordinateur/tablette pour écouter un formateur et voir des slides. Il n'y a pas suffisamment d'interactivité et de coaching des participants. Pourtant, dans ce monde professionnel en développement permanent, investir dans son capital humain représente un levier crucial d'amélioration de la performance des entreprises. À cet égard, la formation et la qualification professionnelles représentent des leviers de développement hautement efficaces, permettant notamment aux professionnels d'affiner leurs compétences ou d'en développer de nouvelles tout en restant informés des nouveautés, toujours plus nombreuses, de leurs domaines d'activité. Comme plusieurs outils de développement professionnel, les méthodes de la certification des personnes ont connu une amélioration nette dans la dernière décennie, surtout avec la digitalisation des services en général et du secteur de la formation en particulier, ce qui a aidé à rendre les services de la formation professionnelle beaucoup plus accessibles.
Que ce soit dans un contexte de crise sanitaire mondiale ou dans un contexte d'usage routinier de la pédagogie, le recours au mode de formation professionnelle en ligne est en augmentation continue et ce, pour plusieurs raisons :

- Ce mode de formation aide l'apprenant à vivre une expérience utilisateur unique et interactive, tout en s'adaptant à ces besoins et à son rythme

- La formation en ligne offre actuellement un avantage par rapport à la formation présentielle puisqu'elle ne demande pas au participant de se déplacer

- Les méthodes du Digital Learning ne cessent de s'améliorer, en offrant des nouveaux outils d'apprentissage créatifs, avec des contenus enrichis et des méthodes d'apprentissage nouvelles que le mode « classique » ne permet pas de mettre en œuvre facilement dans un environnement traditionnel

- Le processus d'apprentissage est facile et garantit une grande valeur ajoutée similaire à celle de la formation en mode présentiel, mais offre finalement plus de flexibilité tant au niveau des horaires (à temps choisi) que de celui de la logistique de la formation elle- même (tout est centralisé au même endroit).

LE MOT DU CEO

Les années qui viennent de s'écouler ont démontré, s'il en était encore besoin, que la pédagogie digitale dans laquelle l'industrie s'essayait depuis des lustres devait nécessairement évoluer pour s'adapter plus efficacement aux défis générés par le recours de plus en plus massif aux méthodes et techniques de formation à l'aide des outils numériques, le système traditionnel de formation en ligne ne répondant en effet plus adéquatement aux nouveaux besoins issus de la dynamique pédagogique numérique que les circonstances ont générée et dont l'évolution est accentuée par le recours massif au télétravail, aux réunions à distance et à l'ultra flexibilité demandée aux usagers de ces modes de travail renouvelés.

C'est le constat que nous avions fait lorsque, au printemps 2020, en plein confinement, nos équipes ont remis sur la table un projet de « pédagogie digitale » que nous envisagions de développer depuis déjà fort longtemps dans le cadre de nos activités de certification des compétences et qui était resté dans les cartons par manque de temps, de focus ou que sais-je encore.

la, il fallait se retrousser les manches et mettre enfin sur les fonts baptismaux ce concept, que nous voulions innovant, pour compléter de manière flexible et efficace le dispositif de certification de personnes qui existait déjà chez **Certi-Trust.**

Nous voulions en effet avant tout, à travers cette proposition de valeur, proposer aux apprenants candidats à la certification de leurs compétences, un apprentissage en ligne qui soit plus flexible tout en étant aussi riche que possible comme il peut l'être dans une salle de classe.
Ayant moi-même une formation pédagogique et ayant œuvré en tant que formateur dans plusieurs domaines depuis plus d'une vingtaine d'années.
j'ai été rapidement convaincu de la nécessité de mettre en place un dispositif hybride entre les pédagogies classique et numérique tout en offrant aux apprenants des programmes de formation évolutifs et graduels qui répondent à leurs besoins de validation de compétences et à leurs contraintes de vie privée ou professionnelle d'une façon relativementinédite.
Ainsi est né « Certi-Trust Digital Learning », presque sur un coin de table, issu de la volonté de nos experts pédagogiques et techniques de proposer une vraie alternative à la traditionnelle formation « en présentiel », chère à tous mais difficilement accessible en raison des conditions très aléatoires de l'époque et c'est sur base de cette dynamique que nous avons créé cette plateforme de « Pédagogie Digitale Augmentée », un système d'apprentissage unique et innovant basé sur la richesse des contenus, la variété des méthodes d'apprentissage et la technologie.

Le leitmotiv de « CTDL » est ainsi devenu, en écho à notre slogan d'entreprise, « Confiance dans l'apprentissage numérique ».

C'est cette plateforme de Digital Learning que je vous invite, à travers la lecture de ce nouveau catalogue de formations certifiantes, à découvrir prochainement et à utiliser pour satisfaire, au mieux de ce que la technologie peut aujourd'hui proposer, les besoins de certification de votre organisations et de vos collaborateurs.
Au plaisir de vous retrouver très prochainement sur : education.certi-trust.online.

Dr Omar Benaicha (CEO Africa & Middle East)

Certi-Trust Digital learning platform

Une plateforme qui combine les avantages des formations présentielles à celles disponibles en ligne.

Découvrez ses principes pédagogiques !

Le contenu nécessaire pour se préparer à la certification (cours, exercices, examen à blanc) est disponible sur la plateforme 24/24, 7j/7 Pendant un an Ce contenu minimum est complété par des dispositifs de partage d'expériences des formateurs Certi-Trust Digital Learning permettant à l'apprenant de mettre en application très rapidement et de manière concrète les apprentissages théoriques.
L'examen se déroule entièrement en ligne, en fonction des disponibilités de l'apprenant.
L'apprenant est totalement engagé et stimulé à travers du contenu interactif, des jeux, différents types d'exercices, des cas d'études concrets inspirés d'expériences vécues et des capsules micro-learning impactantes.
Les dispositifs de communication déployés enrichissent et personnalisent l'expérience utilisateur.

Pack de formation

- Support de cours
- Glossaire
- Exercices QCM
- Exercices ouverts
- Notes et références
- Examen à blanc
- Examen certifiant

NOS EXAMENS DE CERTIFICATION

Dans le cadre de nos activités de validation des compétences professionnelles, nous proposons aux candidats à la certification d'évaluer leur compétence en passant un ou plusieurs examens certifiants correspondant aux schémas sur lesquels ils souhaitent obtenir leur certification. Ces examens sont développés et maintenus par des professionnels expérimentés, certifiés eux-mêmes sur chacun des schémas auxquels ils contribuent dans le cadre de notre politique de gestion des examens (disponible sur le site web de Certi-Trust, partie « Certification de personnes Nos Examens ».
Ils font par ailleurs l'objet d'un renouvellement régulier et d'une actualisation des questions pour coller au plus près de la réalité des domaines techniques ou fonctionnels auxquels ils se rapportent.
Ainsi, au moins 15% des questions de chacun de nos examens sont renouvelées tous les 3 mois pour offrir aux candidats à la certification une expérience de validation de leurs compétences qui soit la plus proche possible de ce que requiert « le terrain ».
D'autre part, nos examens sont souvent disponibles en plusieurs langues (et toujours en Français et en Anglais), permettant ainsi de sélectionner la langue que le candidat maîtrise le mieux pour se faire tester. Et, cerise sur le gâteau, si un candidat échoue malheureusement à l'un de nos examens, il a la possibilité de le repasser GRATUITEMENT dans l'année qui suit, au moment de son choix.
Il est également à noter que, dans le cadre d'une saine gestion de l'impartialité, les examens Certi-Trust sont accessibles à tout un chacun sans qu'il ne soit à priori nécessaire d'avoir suivi une formation spécifique préalablement à leur passage.
Tout candidat peut ainsi choisir d'uniquement se faire tester sans avoir pour autant complété d'autres étapes préalables.
Précisons, à toutes fins utiles, que ceci ne signifie pas que nous ne recommandions pas aux candidats à nos examens de s'y préparer et de disposer des prérequis nécessaires à l'obtention de la certification qui suit ces évaluations car, bien entendu, la simple réussite d'un examen ne suffit pas pour être certifié chez Certi-Trust ... l'expérience professionnelle compte également de manière significative pour obtenir les grades de certification correspondant aux compétences mesurées initialement par l'examen.

PASSEZ VOS EXAMENS EN LIGNE,QUE CE SOIT AU BUREAU OU CHEZ VOUS!

Qui dit examen dit questionnaire ... Notre plateforme "Certi-Trust Advanced System for Online Assessment System», disponible aux candidats inscrits via https://examination.certi-trust.com, constitue le point d'entrée de notre système d'évaluation des compétences.
Sur cette plateforme, le candidat est encadré depuis son inscription jusqu'à la réalisation
effective de ses examens de certification en passant par la procédure de surveillance en ligne (automatisée ou supervisée par un surveillant de Certi-Trust).
Le système d'évaluation propose des questionnaires interactifs similaires à ceux que le candidat aura pu expérimenter sur la plateforme de Digital Learning, lui permettant ainsi de s'y retrouver facilement et de prendre ses marques rapidement pour une expérience qui reste très souple et agréable malgré l'enjeu.

Sécurité de l’information & Cybersécurité

Sécurité de l’information

La sécurité de l’information est essentielle pour protéger les données et garantir leur confidentialité, leur intégrité et leur disponibilité. Développer les compétences dans ce domaine permet aux organisations de maîtriser les risques, de renforcer leur gouvernance et de répondre aux exigences réglementaires.

Cybersécurité

Face à l’évolution constante des cybermenaces, la cybersécurité est devenue un enjeu stratégique pour les organisations.

Développer les compétences dans ce domaine permet de prévenir les cyberattaques, de renforcer la résilience des systèmes d’information et de protéger les actifs numériques.



ISO 27001 Foundation

Cette formation de 21 heures offre aux participants l’occasion de monter en compétence sur la mise en œuvre d’un programme de gestion des risques en sécurité de l’information et de se préparer par la pratique à mener un projet de mise en œuvre d’un programme de gestion des risques conforme à la norme ISO/CEI 27005 : 2018 selon une méthode éprouvée. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l’autorisant à identifier, analyser, évaluer et traiter les risques dans le respect des exigences de l’ISO 27005 et de ses principaux processus. Sur base d’exemples réels et d’exercices concrets,participant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques en sécurité de l’information tout en développant des capacités en gestion de programmes et de méthodes d’appréciation et de traitement ainsi qu’en ce qui concerne la gestion d’équipe, à travers la communication avec les différentes parties intéressées.

Public cible

- Security Officers
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au SMSI dans une organisation
- Dirigeants d’une entreprise souhaitant se familiariser avec les aspects de Sécurité de l’information
- Membres d’une équipe projet en sécurité de l’information
- Opérateurs en technologie de l’information Membre du personnel d’une organisation voulant se préparer pour un poste en sécurité de l’informatio

Objectifs

- Comprendre les enjeux du management de la sécurité de l’information et sa mise en œuvre
- Acquérir la terminologie et les connaissances de base nécessaires pour répondre aux exigences de l’ISO 27001 dans le contexte d’une entreprise
- Découvrir les bonnes pratiques de management de la sécurité de l’information et son articulation avec la gestion des risques
- Réussir l’examen de CERTI-TRUSTTM
- Solliciter la qualification de Certified ISMS Foundation.

Prérequis

Aucun prérequis particulier n’est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties.
À l’issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits). L’examen remplit l’ensembl des exigences
du programme de certification CERTI-TRUSTTM

Programme détaille

Le SMSI tel qu’exigé par la norme ISO/CEI 27001:2022- 7H
Système de Management de la sécurité de l’information – concepts de base
- Principes fondamentaux de la sécurité de l’information
- Les clauses 4 à 10 de l’ISO 27001 et l’Annexe A d’ISO 27001
- Le contexte du SMSI au sein de l’entreprise et son champ d’application
- Aspects de leadership et engagement managérial
- Planification d’un SMSI (gestion des risques, mesures de sécurité, applicabilité, etc.)
- Support des opérations d’un SMSI (documentation, ressources, etc.)

Fonctionnement du SMSI - 7H
- Gestion des opérations d’un SMSI
- Surveillance du SMSI (journalisation, audit et revue de direction)
- Évaluation de l’efficacité des opérations et gestion des métriques
- Actions correctives et amélioration continue
- Processus de certification ISO 27001
- Présentation de la documentation nécessaire aux opérations du SMSI (toolbox)

Examen certifiant « ISMS Foundation »
- 1h, 50 questions (QCM à livre fermé)



ISO 27001 LEAD IMPLEMENTER

Cette formation de 35 heures offre aux participants tl'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre de la gestion de la sécurité de l'information et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise.
Au cours de cette formation, l'étudiant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir l'intégrité du SMSI dans le respect des exigences de la norme ISO 27001 V 2022 ainsi que le processus d'assurance qualité requis par les guides depratiques associés. Sur base d'exemples réels et d'exercices concrets, participant sera amené durant la formation à mener à bien un projet d'implémentation de SMSI en développant des capacités en gestion de programmes et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Security Officer
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un système de management de la Sécurité de l'Information
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information

Objectifs

- Comprendre les principes de fonctionnement d'un SMSI selon l'ISO 27001 V 2022.
- Développer les aptitudes nécessaires pour mener à bien un projet d'implémentation ISO 27001 dans le respect des exigences de la norme et les lignes directrices des normes ISO 27002, 27003, 27004 et 27005.
- Acquérir la compétence de gestion d'une équipe projet pour lancer et maintenir un SMSI.
- Réussir l'examen de CERTI-TRUST™.
- Solliciter la qualification de Certified ISMS Lead Implementer selon le niveau d'expérience.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2022 - 7H
Pour plus d'information, voir le programme détaillé de la formation ISMS Foundation.
Fonctionnement du SMSI – 7H
Pour plus d'information, voir le programme détaillé de la formation ISMS Foundation.
Examen certifiant « ISMS Foundation » • 1h, 50 questions QCM à livre fermé
Préparation et démarrage d'un projet SMSI - 7H
• Les jalons et le calendrier d'un projet de SMSI • Planification d'un projet SMSI
• Périmètre du projet et définition du champ d'application du SMSI
• Les acteurs du projet – Rôles et responsabilités des parties prenantes
• Business Case et méthodologie de gestion de projet
• Obtenir le soutien des parties prenantes et de la direction
• Gestion des relations avec les parties intéressées durant le projet d'implémentation
• Documentation du SMSI • Politiques et procédures du SMSI
• Présentation et utilisation des outils de préparation au projet (via étude de cas)
Les opérations et la performance d'un SMSI - 7H
• Gestion des risques en Sécurité de l'Information
• Mesures de sécurité et sélection des contrôles applicables
• Déclaration d'Applicabilité (DdA) et Plan de traitement des risques (PTR)
• Rôles et responsabilités des opérateurs et des parties intéressées
• Communication, sensibilisation et formation • Gestion des incidents de sécurité
• Surveillance, mesure, analyse et évaluation du SMSI
• Présentation et utilisation des outils de réalisation et de suivi du projet (via étude de cas)
Cycle de vie et pérennité du SMSI - 7H
• Audit interne du SMSI, gestion de la conformité
• Revue de Direction
• Gestion de l'amélioration continue & actions correctives et préventives • Processus de certification
• Présentation et utilisation des outils de suivi du cycle de vie du SMSI (via étude de cas)
Examen certifiant « ISMS Practitioner »
2 H, 100 questions (QCM à livre fermé)



ISO 27001 LEAD AUDITOR

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction d'assurance de la gestion de la sécurité de l'information et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise.
Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser divers types d'audits de 1e, 2e ou 3e partie dans le respect des exigences de la norme ISO 19011 ainsi que le processus de certification requis par la norme ISO 17021.
Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, participant sera amené durant la formation à mener à bien un audit de SMSI en développant des capacités en gestion de programmes et de techniques d'audit ainsi qu'en gestion d'équipe, à travers la communication avec le client d'audit.

Public Cible

- Auditeurs internes
- Auditeurs cherchant à réaliser et à mener des audits dans les systèmes de sécurité d'informations
- Gestionnaires de projets ou consultants souhaitant maîtriser les audits des systèmes de sécurité d'informations
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information

Objectifs

- Comprendre les principes de fonctionnement d'un SMSI selon l'ISO 27001 2022.
- Développer les aptitudes nécessaires pour mener à bien un audit ISO 27001 dans le respect des exigences de ISO 19011 et les spécifications de l'ISO 17021 et l'ISO 27006
- Acquérir la compétence de gestion d'une équipe d'auditeurs de SMSI
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISMS Lead Auditor selon le niveau d'expérience.

Prérequis

Une connaissance de base de la sécurité de l'Information et de la norme ISO 27001 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2022 - 7H
Pour plus d'information, voir le programme détaillé de la formation ISMS Foundation.
Fonctionnement du SMSI – 7H
Pour plus d'information, voir le programme détaillé de la formation ISMS Foundation.
• Examen certifiant « ISMS Foundation » 1h, 50 questions QCM à livre fermé
Préparation et démarrage d'un projet SMSI - 7H
• Concepts de base, principes et critères d'audit selon ISO 19011
• Déroulement général d'un audit de SMSI • Audits interne et externe • Les acteurs de l'audit
• Planification et mise en œuvre d'un programme d'audit
• Activités préparatoires à l'audit, gestion des relations avec l'audité avant et pendant l'audit
• Documentation de l'audit • Audit documentaire (audit d'étape 1)
• Présentation et utilisation des outils de préparation à un audit (via étude de cas)
Réalisation de l'audit sur site d'un SMSI – 7H
• Préparation de l'audit sur site (audit d'étape 2)
• Approche d'audit fondée sur la preuve et les risques
• Les différentes procédures d'audit
• Création de plans de test d'audit
• Exercices pratiques : simulations d'entretiens et de collecte de preuve
• Aspects liés aux rapports d'audit
• Revue de qualité des constats d'audit et préparation des conclusions
• Présentation et utilisation des outils de réalisation d'un audit (via étude de cas)
Clôture et suivi de l'audit – 7H
• Présentation des conclusions • Réunion de clôture
• Rédaction du rapport d'audit
• Suites à l'audit du SMSI (plans d'action et suivi de ceux-ci)
• Audits de surveillance et de suivi
• Présentation et utilisation des outils de reporting d'un audit (via étude de cas pratique)
Examen certifiant « ISMS Auditor»
2 heures , 100 questions QCM à livre fermé.



ISO 27005 RISK MANAGER

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la mise en œuvre d'un programme de gestion des risques en sécurité de l'information et de se préparer par la pratique à mener un projet de mise en œuvre d'un programme de gestion des risques conforme à la norme ISO/CEI 27005 : 2018 selon une méthode éprouvée. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à identifier, analyser, évaluer et traiter les risques dans le respect des exigences de l'ISO 27005 et de ses principaux processus. Sur base d'exemples réels et d'exercices concrets, participant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques en sécurité de l'information tout en développant des capacités en gestion de programmes et de méthodes d'appréciation et de traitement ainsi qu'en ce qui concerne la gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Security Officer
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un système de management de la Sécurité de l'Information
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information

Objectifs

- Comprendre la relation entre la gestion des risques en sécurité de l'information et les mesures de sécurité associées
- Assurer une gestion efficace des risques, à travers les concepts, approches, méthodes et techniques selon l'ISO 27005
- Développer des aptitudes sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISMS Risk
- Manager selon le niveau d'expérience.

Prérequis

Une connaissance de base de la Sécurité de l'Information et de la norme ISO 27001 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 21 heures, réparties sur 3 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 21 CPE (Continuous Professional Education credits)

Programme Détaille

Programme de gestion des risques selon la norme
- ISO/CEI 27005 : 2018 – 7H
- Gestion des risques en sécurité de l'information concepts & principes fondamentaux
- Le cadre normatif de la gestion des risques
- La norme ISO/CEI 27005 : 2018
- Planification de la gestion des risques
- Le contexte de l'organisation et le périmètre de gestion des risques
- Mise en œuvre d'un programme de gestion des risques
- Approches de la gestion des risques
- Présentation de différentes méthodes de gestion des risques (toolbox)

Appréciation et traitement du risque en sécurité de l'information - 7H
- Identification des risques
- Analyse des risques
- Évaluation des risques
- Traitement du risque
- Relations entre ISO 27005 et ISO 27001
- Présentation et utilisation d'outils pratiques de gestion des risques (via étude de cas)

Activités de soutien et de surveillance des risques - 7H
- Documentation de la gestion des risques
- La communication sur le risque
- Les métriques d'évaluation de l'efficacité de la gestion des risques
- La réévaluation du risque
- L'amélioration continue de la gestion du risque
- Présentation et utilisation d'outils pratiques de gestion des risques (via étude de cas)

Examen certifiant « ISMS Risk Manager »
- 2h,100 questions QCM à livre fermé



EBIOS RISK MANAGER

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la mise en œuvre d'un programme de gestion des risques en sécurité de l'information et de se préparer par la pratique à mener un projet de mise en œuvre d'un programme de gestion des risques selon la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité). Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à identifier, analyser, évaluer et traiter les risques dans le respect de la structure méthodologique propres à EBIOS et ses principaux processus. Sur base d'exemples réels et d'exercices concrets, l'étudiant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques en sécurité de l'information tout en développant des capacités en gestion de cette méthode d'appréciation et de traitement des risques en sécurité de l'information ainsi qu'en ce qui concerne la communication avec les différents intervenants

Public Cible

- Officiers de sécurité
- Gestionnaires de risque
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre de la méthodologie
- EBIOS en entreprise
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information ou de RSSI

Objectifs

- Comprendre le déroulement d'une approche en gestion des risques en sécurité de l'information basée sur EBIOS et les mesures méthodo logiques associées
- Assurer une gestion technique efficace des risques à travers la méthode EBIOS
- Développer des aptitudes sur l'exécution de la méthode à travers des cas pratiques de gestion des risques liés à la sécurité de l'information
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified EBIOS Risk
- Manager selon le niveau d'expérience.

Prérequis

Une connaissance de base de la Sécurité de l'Information et de la norme ISO 27005 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 21 heures, réparties sur 3 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 21 CPE (Continuous Professional Education credits)

Programme Détaille

Introduction à la méthode EBIOS - 7H
- Gestion des risques en sécurité de l'information concepts & principes fondamentaux
- Cadre normatif de la gestion des risques
- La méthode EBIOS – Introduction, principes et concepts de base
- Les 5 phases de la méthode EBIOS
- Définition du cadre de la gestion des risques
- Identification des menaces, vulnérabilités, biens essentiels et biens de support
- Critères de sécurité et échelles de besoins, gravité et vraisemblance
- Appréciation des scénarios de menace

Réalisation de l'appréciation des risques avec EBIOS - 7H
- Analyse des risques
- Évaluation des risques
- Identification des objectifs de sécurité
- Choix des options de traitement du risque
- Relations entre ISO 27005 et EBIOS
- Formalisation des mesures de sécurité à mettre en œuvre

Activités de soutien et de surveillance des risques - 7H
- Exécution des traitements sur les risques
- Mise en oeuvre des mesures de sécurité
- Élaboration des plans d'action
- Analyse des risques résiduels
- Homologation de sécurité
- Cas pratique de gestion des risques (via étude de cas complète)

Examen certifiant « EBIOS Risk Manager »
2h – 100 questions QCM à livre fermé



CYBERSECURITY FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la cybersécurité et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet d'un NIST au sein de l'organisation. Au cours de cette formation, participant acquerra les bases de connaissances et certaines aptitudes lui permettant de comprendre le cadre de Cybersécurité du NIST. Objectifs Comprendre les enjeux du management de la cybersécurité et sa mise en œuvre Acquérir la terminologie et les connaissances de base liées à la cybersécurité dans le contexte d'une entreprise. Découvrir les bonnes pratiques de la cybersécurité et son articulation avec la sécurité de l'information et la gestion des risques Réussir l'examen de CERTI-TRUST™ Solliciter la qualification de Certified cybersecurity Foundation. Sur base de cas d'exemples et d'exercices pratiques, participant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un programme en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles-ci dans une perspective de maîtrise des enjeux liés à la cybersécurité de leur organisation.

Public Cible

- IT Security Officers
- Gestionnaires de SoC
- Responsables des actifs digitaux d'une organisation
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un programme de gestion de la Cybersécurité
- Managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques en Cybersécurité
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en Cybersécurité

Objectifs

- Comprendre les enjeux du management de la cybersécurité et sa mise en œuvre
- Acquérir la terminologie et les connaissances de base liées à la cybersécurité dans le contexte d'une entreprise.
- Découvrir les bonnes pratiques de la cybersécurité et son articulation avec la sécurité de l'information et la gestion des risques
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified cybersecurity Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

Cette formation dure 14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).

Programme Détaille

Le programme de Cybersécurité selon le NIST Cybersecurity Framework -7H
- Concepts et principes de base en Cybersécurité
- Cadre légal et normatif en Cybersécurité
- Le NIST Cybersecurity Framework
- Organisation et clarification des objectifs de la cybersécurité
- Analyse du contexte existant et de l'exposition
- Déclencheurs d'un programme de Cybersécurité
- Outils de support d'un programme de Cybersécurité (documentation, ressources, etc.)

Cyberattaques et exposition des organisations - 7H
- Threat Intelligence et évaluation des risques
- Vecteurs d'attaque communs, agents de menaces, motifs et types d'attaques
- Surveillance du programme de Cybersécurité
- Les incidents en Cybersécurité, leurs conséquences et la réponse à y apporter
- Gestion de crise et des urgences, niveaux de préparation
- Présentation de la documentation nécessaire aux opérations du programme (toolbox)

Examen certifiant « Cybersecurity Foundation »
(1h-50 questions QCM à livre fermé)



CYBERSECURITY LEAD IMPLEMENTER

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre de la gestion d'un programme de Cybersécurité et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participantacquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir l'intégrité du programme de Cybersécurité dans le respect des meilleures pratiques du NIST ainsi que des normes internationales associées. Sur base de labs pratiques, d'exemples réels et d'exercices concrets basés sur des environnements à simulation technique avancée, participant sera amené durant la formation à mener à bien un projet d'implémentation d'un programme de Cybersécurité en développant des capacités en identification des menaces, en gestion de programmes, de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées dans le Cyberspace.

Public Cible

- IT Security Officers
- Gestionnaires de SoC
- Responsables des actifs digitaux d'une organisation
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un programme de gestion de la Cybersécurité
- Managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques en Cybersécurité
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en Cybersécurité

Objectifs

- Maîtriser les concepts, approches, normes, méthodes et techniques pour participer à la mise en œuvre et la gestion d'un programme de Cybersécurité conforme au référentiel du NIST au sein d'une organisation
- Comprendre le but, le contenu et la corrélation entre la Sécurité de l'Information et le cadre de
- Cybersécurité du NIST ainsi qu'avec d'autres normes
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques de gestion de la cybersécurité
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified Cybersecurity Lead Implementer selon le niveau d'expérience

Prérequis

Des connaissances minimales sur la sécurité de l'information et des concepts connexes sont nécessaires pour la réussite du cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participatio à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le programme de Cybersécurité selon le NIST Cybersecurity Framework - 7H
- Cadre légal et normatif en Cybersécurité
- Le NIST Cybersecurity Framework
- Organisation et clarification des objectifs de la cybersécurité
- Analyse du contexte existant et de l'exposition
- Déclencheurs d'un programme de Cybersécurité
- Outils de support d'un programme de Cybersécurité (documentation, ressources, etc.)
- Cyberattaques et exposition des organisations - 7H • Threat Intelligence et évaluation des risques • Vecteurs d'attaque communs, agents de menaces, motifs et types d'attaques
- Surveillance du programme de Cybersécurité • Les incidents en Cybersécurité, leurs conséquences et la réponse à y apporter
- Gestion de crise et des urgences, niveaux de préparation • Présentation de la documentation nécessaire aux opérations du programme (toolbox)

Examen certifiant «Cybersecurity Foundation» (1h-50 questions QCM à livre fermé)
Planifier et démarrer un programme de Cybersécurité - 7H
- Gouvernance de la Cybersécurité, meilleures pratiques et cadre normatif • Planification du programme de Cybersécurité • Périmètre du programme • Structure organisationnelle de la Cybersécurité, rôles et responsabilités • Gestion des ressources du programme de Cybersécurité
- Gestion de la documentation du programme • Politiques et procédures du programme de Cybersécurité • Compréhension des menaces et gestion des risques « cyber » (LAB) • Présentation et utilisation des outils du programme de Cybersécurité (via LAB)

Les opérations et la performance du programme de Cybersécurité-7H
- Mesures de sécurité et sélection des contrôles applicables • Options de traitement des risques majeurs et continuité opérationnelle
- Rôles et responsabilités des opérateurs et des parties intéressées • Communication, sensibilisation et formation des acteurs
- Gestion des incidents de sécurité et récupération (LAB) • Surveillance, mesure, analyse et évaluation du programme de Cybersécurité
- Présentation et utilisation des outils de réalisation et de suivi du programme (via LAB)

Cycle de vie du programme de Cybersécurité - 7H
- Test du programme de Cybersécurité • Plans d'action, suivi des anomalies et correction des défaillances • Gestion de l'amélioration continue du programme • Processus de certification • Présentation et utilisation des outils de suivi du cycle de vie du programme (via LAB)

Examen certifiant « Cybersecurity Practitioner »
(2h-100 questions QCM à livre fermé)



CLOUDSECURITY FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la sécurité du cloud et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet d'un programme de sécurité du Cloud basé sur ISO 27017 et ISO 27018. Au cours de cette formation, l'étudiant acquerra les bases de connaissances et certaines aptitudes lui permettant de comprendre les tenants et aboutissants des exigences des normes ISO 27017 et ISO 27018 pour la mise en œuvre et les opérations d'un programme de la sécurité du cloud. Sur base de cas d'exemples et d'exercices pratiques, l'étudiant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un programme en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles-ci dans une perspective de maîtrise des enjeux liés à la Sécurité du cloud de leur organisation.

Public Cible

- Professionnel voulant à s'initier à la sécurité du cloud.
- IT Security Officers
- Gestionnaires de plateformes digitales hébergées dans le Cloud
- Responsables des actifs digitaux d'une organisation
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un programme de gestion de la sécurité du Cloud
- Managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques de sécurité liés au Cloud computing
- Membres d'une équipe de sécurité de l'information
- Administrateurs systèmes et ingénieurs voulant se préparer pour un poste en relation avec la sécurité du Cloud computing

Objectifs

- Comprendre les enjeux du management de la sécurité du cloud et sa mise en œuvre
- Acquérir la terminologie et les connaissances de base nécessaires pour répondre aux exigences de
- l'ISO 27017 et de L'ISO 27018 dans le contexte d'une entreprise.
- Découvrir les bonnes pratiques demanagement de la sécurité du cloud et son articulation avec la gestion des risques
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified cloudsecurity Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

Cette formation dure 14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. Laparticipation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).

Programme Détaille

Le programme de sécurité du cloud tel que défini par les normes ISO 27017 et ISO 27018 - 7H
- Terminologie et principes de base en sécurité du cloud
- Cadre légal et normatif en sécurité du cloud
- Organisation et clarification des objectifs de la sécurité du Cloud
- Analyse du contexte existant et de l'exposition
- Déclencheurs d'un programme de sécurité du cloud
- Outils de support d'un programme de sécurité du cloud (documentation, ressources, etc.)

Fonctionnement d'un programme de sécurité Cloud + Outils de gestion du cycle de vie d'un programme de sécurité du cloud - 7H
- Mise en œuvre d'un programme de sécurité du cloud
- Surveillance du programme de sécurité du cloud
- Les incidents en sécurité du cloud, leurs conséquences et la réponse à y apporter
- Gestion de crise et des urgences, niveaux de préparation
- Présentation de la documentation nécessaire aux opérations du programme

Examen certifiant « Cloudsecurity Foundation »
(1h-50 questions QCM à livre fermé)



RÔLE DU RSSI

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction de Responsable de la Sécurité des Systèmes d'Information d'une organisation et de la gestion d'un programme de Cybersécurité ainsi que de se préparer par la pratique à diriger des participants opérationnelles sur base de principes, de référentiels, d'outils et de techniques de gestion de sécurité informatique largement appliqués dans le monde de l'entreprise.
Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à exercer les fonctions de RSSI sur les plans de la Gouvernance, de la gestion des contraintes légales et réglementaires, ainsi qu'en fonction des nécessités techniques liées à cette fonction-clé, dans le respect des meilleures pratiques et des normes internationales associées. Sur base d'exercices pratiques, d'exemples réels et de situations concrètes basés sur des environnements à simulation technique avancée, participant sera amené à envisager son rôle en tant que RSSI en développant ses aptitudes multidisciplinaires en gestion de la mise en œuvre et de suivi de projets de Cybersécurité ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées dans l'entreprise

Public Cible

- RSSI en charge
- Candidat à la fonction de RSSI
- Responsables des actifs digitaux d'une organisation
- Chefs de projets ou consultants souhaitant comprendre les enjeux liés à la sécurité informatique d'une entreprise
- Managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques en
- Cybersécurité
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste de RSSI

Objectifs

- Maîtriser les concepts, approches, normes, méthodes et techniques pour exercer un rôle de premier plan et accompagner la transformation digitale en tant que RSSI au sein d'une organisation
- Comprendre le but, le contenu et la corrélation entre les différentes composantes du rôle à tenir, sur les plans de la Gouvernance et de la gestion opérationnelle ou technique
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques de gestion de la Cybersécurité et de la sécurité de l'information
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de RSSI Certifié selon le niveau d'expérience.Cybersecurity Lead Implementer selon le niveau d'expérience

Prérequis

Des connaissances minimales sur la sécurité de l'information et des concepts connexes sont nécessaires pour la réussite du cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Gouvernance SSI – partie 1 : La gouvernance globale de la SSI (7 H)
• Concepts et principes de base en Sécurité de l'Information • Cadre normatif de base • Établissement du contexte et des enjeux de Sécurité de l'Information • Structuration de la filière SSI au sein d'une organisation • Pilotage de la sécurité des systèmes d'information et Cybersécurité • Aspects de sensibilisation et de formation à la sécurité des systèmes d'information

Gouvernance SSI – partie 2 : La gestion des risques (7 H)
• Vecteurs d'attaque communs, agents de menaces, motifs et types d'attaques • Évaluation des risques SSI • Traitement des risques SSI Les incidents en Cybersécurité, leurs conséquences et la réponse à y apporter • Gestion de crise et des urgences, niveaux de préparation

Gouvernance SSI - partie 3: Gérer la sécurité opérationnelle (7 H)
• Gouvernance de la SSI et application des meilleures pratiques • Politiques et procédures à mettre en œuvre pour encadrer la SSI • Surveillance et mesure de l'efficacité d'un programme SSI (KPI's et tableaux de bord) • Encadrer et piloter la sécurité des réseaux et des systèmes • Sécurité du contrôle d'accès et gestion des identités • Aspects de sécurité applicative La cryptographie et son bon usage dans le cadre d'une gestion cohérente de la SSI • Audits interne et externe des systèmes d'information • Le SOC (Security Operations Center ou Cellule de SécuritéOpérationnelle)

Aspects légaux de la SSI (7 H)
• Les bases du droit (hiérarchie des normes, responsabilité, sanctions, …) • Aspects de responsabilité légale du RSSI • Panorama du cadre réglementaire (y compris Loi informatique et libertés et RGPD) • Investigation, collecte et gestion de la preuve numérique • Légalité du contrôle au sein de l'entreprise (surveillance, accès au poste de travail, …) • Accessibilité et opposabilités des moyens télécoms
• Suivi des anomalies et intrusions, dépôts de plaintes

La Cybersécurité opérationnelle par l'exemple (7 H)
• Présentation des menaces et des vecteurs d'attaques les plus communs et solutions pour s'en prémunir • Anatomie d'une attaque réussie (exemples cas réels) • Virtualisation des systèmes d'information et Sécurité du Cloud • Hardening de systèmes d'information (Windows et Linux)

Examen « RSSI Certifié »
(3h-100 questions QCM et 1 question ouverte)
Threat Intelligence et appréciation des risques SSI



HDS FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de l'hébergement des données de santé et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du HDS dans le monde de l'entreprise.
Au cours de cette formation, participant acquerra les bases de connaissance et certaines aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de l'hébergement des données de santé. Sur la base de cas d'exemples et d'exercices pratiques, l'étudiant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un HDS en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles-ci dans une perspective de maîtrise des enjeux liés à l'hébergement de vos données de santé.

Public Cible

- Infogéreurs
- Hébergeurs
- Professionnels du secteur de la santé
- Spécialistes en protection des données
- Professionnels voulant s'initier aux techniques exigées par le référentiel HDS

Objectifs

- Comprendre les questions de gestion de la
- sécurité de l'information relatives aux données de santé.
- Acquérir la terminologie et les connaissances de base pour remplir les exigences du référentiel HDS.
- Découvrir les bonnes pratiques de gestion pour la sécurité de l'information des données de santé.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified HDS Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à la formation conduisant à cette certification.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux apprenants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Jour 1 : Introduction (HDS : de l'agrément à la certification)
- Sources législatives • Pourquoi le HDS ?
- Quel est son périmètre / son champ d'application ?
- Information et données
- Cycle de vie de l'Information • Gestion de l'information
- Sécurité de l'Information • Tendances et statistiques
- Confidentialité, intégrité et disponibilité • Processus et actifs principaux
- Actifs secondaires
- Principes de protection des actifs • Raisons pour implémenter un SMSI
- Fonctionnement du SMSI • Planification et contrôle opérationnels
- Objectifs, natures & catégories des mesures de
- sécurité de l'information • Contrôle de l'environnement du SMSI
- Mesures des 14 domaines de sécurité expliqués du SMSI

Jour 2 : Les exigences du HDS et les moyens d'y répondre + L'audit de certification
- Référentiel de certification HDS • Exigences de l'ISO 27001 • Exigences de l'ISO 20000
- Exigences relatives à la protection des données à caractère personnel
- Exigences complémentaires
- Choix du domaine d'application • Référentiel d'accréditation HDS
- Qu'est-ce qu'un audit ?
- Types d'audits • Les acteurs de l'audit • Processus général d'audit
- Processus de réalisation d'un audit de certification HDS
- Objectifs de l'audit en général et de l'audit HDS en particulier
- Contrat de certification
- Processus de certification
- Durée d'un audit HDS
- Constats d'audit et non-conformités
- Processus de certification HDS
- Résumé de la formation et leçons apprises
- Révision des concepts-clés
- Examen et processus de certification
- Évaluation de la formation Au revoir

Examen certifiant « HDS Foundation »
1h, 50 questions QCM à livre fermé

Intelligence artificielle & gouvernance IA

L'intelligence artificielle transforme profondément les modèles économiques, les processus métiers et les modes de décision des organisations.
Si elle offre de nombreuses opportunités en matière d'innovation, de performance et d'automatisation, son déploiement nécessite une gouvernance rigoureuse afin de garantir une utilisation responsable, éthique, sécurisée et conforme aux exigences réglementaires.
Développer les compétences en gouvernance de l'IA permet aux organisations d'identifier et de maîtriser les risques, de renforcer la confiance des parties prenantes et de favoriser une adoption durable et maîtrisée des technologies d'intelligence artificielle.

CERTIFIED AI PROFESSIONAL (CAIP)
ISO/IEC 42001 LEAD IMPLEMENTER

Cette formation certifiante de 35 heures vise à doter les professionnels des compétences techniques, stratégiques et réglementaires nécessaires pour piloter efficacement des projets IA.

Public Cible

- Directeurs généraux et décideurs stratégiques
- Responsables innovation & transformation digitale
- Risk managers & compliance officers
- Responsables IT & data
- Consultants et auditeurs
- Chefs de projets

Objectifs

- Comprendre les fondamentaux de l'Intelligence Artificielle et du Machine Learning
- Identifier les opportunités d'intégration de l'IA dans leur organisation
- Piloter un projet IA de bout en bout
- Évaluer les risques, biais algorithmiques et enjeux éthiques
- Intégrer les exigences réglementaires (AI Act, RGPD, gouvernance des données)
- Mettre en place une stratégie IA responsable et performante

Prérequis

Connaissances générales en management ou en systèmes d'information
Aucune compétence technique avancée en programmation n'est requise

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Fondamentaux de l'IA – 7H
Histoire et évolution de l'IA
Machine Learning, Deep Learning, NLP
Cas d'usage sectoriels
Limites et risques de l'IA
Data & Modèles IA – 7H
- Cycle de vie d'un projet IA
- Qualité et gouvernance des données
- Types de modèles (supervisé, non supervisé, génératif)
- Introduction aux modèles comme OpenAI et aux LLM

Cadre réglementaire & IA responsable – 7H
- Cadre réglementaire international
- Focus sur le AI Act
- Articulation avec le Règlement général sur la protection des données (RGPD)
- Gestion des biais et discrimination algorithmique
- IA responsable & ESG

Gestion des risques & sécurité – 7H
- Cartographie des risques IA
- Cybersécurité et IA
- IA & conformité
- Audit des systèmes d'IA

Stratégie & implémentation – 7H
- Élaboration d'une roadmap IA
- ROI & indicateurs de performance
- Conduite du changement
- Atelier pratique : conception d'un plan IA organisationnel

Examen certifiant « Certified AI Professional »

ISO/IEC 42001 LEAD AUDITOR

Cette formation de 35 heures prépare les participants à auditer des systèmes de management de l'intelligence artificielle (SMIA), depuis les fondamentaux de l'IA jusqu'à la conduite complète d'un audit ISO/IEC 42001. Les participants y acquièrent d'abord une compréhension solide des concepts clés de l'IA, avant d'aborder le cadre normatif de la norme et les fondamentaux de l'audit. La formation se conclut par la conduite pratique d'un audit complet. À l'issue de la formation, les participants sont en mesure de planifier, mener et clôturer un audit ISO/IEC 42001 en autonomie.

Public Cible

- Auditeurs internes ou externes souhaitant se spécialiser dans l'audit des systèmes de management de l'IA
- Managers, consultants ou conseillers experts en management de l'IA
- Responsables de la conformité aux exigences d'un système de management de l'IA
- Professionnels impliqués dans le développement, la mise en œuvre ou l'architecture de systèmes d'IA

Objectifs

- Comprendre les principes d'un système de management de l'IA selon l'ISO/IEC 42001
- Évaluer la conformité d'un SMIA aux exigences de la norme, du point de vue d'un auditeur
- Planifier, mener et clôturer un audit ISO/IEC 42001, selon l'ISO/IEC 17021-1 et l'ISO 19011
- Gérer un programme d'audit ISO/IEC 42001

Prérequis

Une compréhension fondamentale de l'ISO/IEC 42001 ainsi que des principes et concepts de l'intelligence artificielle est nécessaire pour participer à cette formation.

Durée

Cette formation se déroule sur 5 jours, incluant l'examen de certification le dernier jour. Un certificat de participation est remis à l'issue de la formation. La participation à cette formation donne droit à 35 crédits CPD (Continuing Professional Development).

Programme Détaille

Fondamentaux de l'IA - 7H
- Histoire et évolution de l'IA
- Machine Learning, Deep Learning, NLP
- Cas d'usage sectoriels
- Limites et risques de l'IA
- Cadre réglementaire international (focus sur l'AI Act et le RGPD)
- Gestion des biais et discrimination algorithmique

Cadre normatif et fondamentaux de l'audit d'un SMIA - 7H
- Analyse du contexte de l'entreprise au regard des enjeux de l'IA (chapitre 4)
- Politique de management de l'IA, rôles et responsabilités (chapitre 5)
- Évaluation des risques de l'IA et des impacts du SMIA (chapitre 6)
- Mise en œuvre et maîtrise opérationnelle du SMIA (chapitres 7 & 8)
- Évaluation et amélioration continue du SMIA (chapitres 9 & 10)
- Fondamentaux de l'audit : déontologie, approche fondée sur la preuve et le risque

Data & modèles : méthodologie et pratique de l'IA - 7H
- Cycle de vie d'un projet IA
- Qualité et gouvernance des données
- Types de modèles (supervisé, non supervisé, génératif)
- Introduction aux LLM (ex. modèles type OpenAI)

Conduite et mise en œuvre d'un audit - 7H
- Déclenchement d'un audit
- Audit d'étape 1
- Audit d'étape 2
- Bonnes pratiques durant les audits
- Recueil et vérification des informations obtenues lors de l'audit d'étape 2

Conduite et mise en œuvre d'un audit – Suite - 7H
- Procédures d'audit, rédaction des constats et rapports de non-conformité
- Clôture d'un audit et certification, activités de surveillance et de suivi
- Compétences et évaluation des auditeurs

Examen certifiant «Certified ISO/IEC 42001 Lead Auditor »
2 heures , 100 questions QCM à livre fermé.

Protection des données Personnelles & Vie privée

Dans un environnement où les données personnelles sont au cœur des activités des organisations, leur protection constitue un enjeu majeur de conformité, de confiance et de responsabilité. La mise en place de bonnes pratiques en matière de protection de la vie privée permet de garantir le respect des droits des personnes, de répondre aux exigences réglementaires et de réduire les risques liés au traitement des données.
Développer les compétences dans ce domaine est essentiel pour intégrer la protection des données dans les processus de l'organisation, renforcer la confiance des parties prenantes et promouvoir une culture de la confidentialité.



RGPD

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la protection des données à caractère personnel et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du RGPD dans le monde de l'entreprise. Au cours de cette formation, participant acquerra la connaissance et les compétences pour comprendre les tenants et aboutissants des exigences du règlement général sur la protection des données

Public Cible

- Chefs de projet ou consultants souhaitant accompagner une organisation dans la mise en œuvre et l'adoption des nouvelles exigences du RGPD
- Les auditeurs qui souhaitent comprendre le RGPD
- Délégués à la Protection des Données et CxO chargés de la protection des données personnelles d'une entreprise et de la gestion de ses risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en protection des données personnelles Avocats, juristes

Objectifs

- Comprendre les enjeux de la protection des données selon le RGPD et sa mise en œuvre.
- Acquérir la terminologie et les connaissances de base nécessaires pour remplir les exigences du RGPD.
- Découvrir les bonnes pratiques de gestion des données personnelles.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified GDPR Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à14 CPE (Continuous Professional Educationcredits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

La Protection des Données et le RGPD - 7H
- Aperçu du cadre international de protection des données
- La protection des données en Europe
- Cadre normatif et meilleures pratiques de management
- Concepts et principes fondamentaux du RGPD
- Aspects de légitimation et droits des personnes
- Focus sur le consentement éclairé
- Soutien documentaire et références au RGPD (documentation, ressources, etc.)

Les composants du RPGD et les relations qu'ils entretiennent - 7H
- Mesures liées à la conformité de la protection des données (politiques, procédures, etc.)
- Les différents intervenants et leurs obligations légales
- Privacy by design & by default – aspects principaux
- Notification et divulgation des failles de sécurité et des pertes de données
- Le Délégué à la Protection des Données (DPD / Data Protection Officer, DPO)
- Les autorités de protection des données et leur rôle
- Transferts internationaux de dotnnées
- Lignes directrices pour l'interprétation du RGPD (le groupe des 29, opinions du EDPB)

Examen certifiant « GDPR Foundation »
- 1h, 50 questions QCM à livre fermé



(DPO) DATA PROTECTION OFFICER

Le nouveau règlement général sur la protection des données (RGPD) est directement applicable dans chaque État membre et conduit à un plus grand degré d'harmonisation de la protection des données. Les responsables du traitement des données et les sous-traitants doivent désigner un délégué à la protection des données (DPD) pour se conformer au règlement. Notre proposition de formation est développée pour préparer les candidats à ce rôle. Ce programme certifiant est conçu dans une double perspective, technologique et juridique, en tenant compte de l'application pratique et des meilleures pratiques et expériences de l'industrie dans des domaines tels que la sécurité, la protection des données personnelles et la gouvernance informatique. Le programme de certification Data Protection Officer a été développé pour, sur base d'exemples réels et d'exercices concrets, donner à participant les connaissances tet aptitude lui permettant de mener à bien la mise en œuvre d'un programme de conformité de la protection des données àcaractère personnel au bénéfice de son organisation.

Public Cible

- Chefs de projet ou consultants souhaitant accompagner une organisation dans la mise en œuvre et l'adoption des nouvelles exigences du RGPD
- Les auditeurs qui souhaitent comprendre pleinement le processus de mise en œuvre du RGPD
- Délégués à la Protection des Données et CxOchargés de la protection des donnée spersonnelles d'une entreprise et de la gestion de ses risques Avocats, juristes
- Conseillers experts en protection des données personnelles
- Experts en conformité souhaitant se préparer à un poste de délégué à la protection des données.

Objectifs

- Acquérir une compréhension globale des concepts, des approches, des méthodes et des techniques pour appliquer efficacement le GDPR/RGPD
- Comprendre les exigences que le GDPR/RGPD impose aux organisations de l'UE et aux organisations hors-UE et acquérir l'expertise nécessaire pour leur mise en œuvre
- Savoir gérer une équipe de protection des données.
- Développer les connaissances et compétences nécessaires pour conseiller les organisations sur les meilleures pratiques en matière d'analyse et de prise de décision concernant la gestion des données personnelles.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified Data
- Protection Officer selon le niveau d'expérience.

Prérequis

Une connaissance de base du Règlement Général sur la Protection des Données de l'UE est recommandée pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

La Protection des Données et le RGPD - 7H
Pour plus d'information voir le programme détaillé de la formation RGPD.
Les composants du RGPD et les relations qu'ils entretiennent - 7H
Pour plus d'information voir le programme détaillé de la formation RGPD.
Examen certifiant « GDPR Foundation »
• 1h, 50 questions QCM à livre fermé
Réglementation par la pratique, gestion des risques et de la conformité - 7H
• Arsenal réglementaire européen en matière de protection des données
• Gestion des risques en matière de protection des données à caractère personnel
• Appréciation des risques en matière de protection des données et mesures applicables
• Mesures de protection et gestion des risques résiduels • Méthodologie de gestion des risques appliquées à une étude de cas (toolbox)
• Aspects de conformité au RGPD • Business Case & méthodologie de mise en œuvre et de gestion d'un projet de conformité
• Traçabilité du modèle de conformité • Relations entre conformité au RGPD, Sécurité de l'Information et Cybersécurité
• Présentation et utilisation des outils de gestion d'un programme (étude de cas)
Appréciation des impacts sur la protection des données (DPIA) - 7H
• Introduction au DPIA, origines, concepts et caractéristiques • Mener une appréciation des impacts aspects préparatoires
• Mettre en œuvre un DPIA (atelier pratique) • Différences entre risques standards et risques élevés pour le sujet
• Le rôle du Délégué à la Protection des Données dans un DPIA
• Gestion du cycle de vie de la protection des données • Références, opinions et recommandations de diverses sources
• Présentation d'outils de gestion et de suivi du DPIA (toolbox et étude de cas)
Assurance du programme de conformité de la protection des données - 7H
• L'audit de la protection des données aspects généraux • Audit des systèmes d'information et intégration de mesures sur la protection des données • Contrôle interne et amélioration continue • Utilisation d'outils de suivi du cycle de vie du programme de conformité (étude de cas)
Examen certifiant « Data Protection Officer »
2h , 100 questions QCM à livre fermé



EXPERT EN PROTECTION DES DONNÉES LOI 09-08

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la protection des données à caractère personnel au Maroc et de maîtriser les exigences de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Elle permet de comprendre en profondeur le cadre légal et réglementaire marocain, les rôles et responsabilités des différents acteurs (responsable de traitement, sous-traitant, CNDP, etc.), ainsi que les bonnes pratiques de conformité à mettre en œuvre dans les organisations publiques et privées. À travers des cas concrets, des mises en situation et des exercices pratiques, les participants apprendront à identifier les risques liés aux traitements de données, à élaborer une cartographie de conformité, et à mettre en place un programme de gouvernance et de conformité à la loi 09-08.

Public Cible

- Délégués à la protection des données (DPO) et correspondants CNDP.
- Responsables juridiques, conformité ou audit interne.
- Responsables sécurité de l'information, RSSI, CISO.
- Consultants et experts en conformité réglementaire.
- Dirigeants et managers souhaitant comprendre leurs obligations légales en matière de protection des données
- Toute personne souhaitant développer une expertise dans la mise en œuvre et la conformité à la loi 09-08.

Objectifs

- Comprendre le cadre juridique marocain en matière de protection des données personnelles (loi 09-08 et textes d'application).
- Identifier les droits des personnes concernées et les obligations des responsables de traitement et sous-traitants.
- Maîtriser le processus de notification etd'autorisation auprès de la CNDP (Commission
- Nationale de Contrôle de la Protection des
- Données à Caractère Personnel).
- Savoir analyser les risques liés aux traitements de données et définir des mesures de conformité.
- Élaborer et piloter un programme de conformité à la loi 09-08 au sein de son organisation.
- Réussir l'examen de CERTI-TRUST™ et obtenir la qualification Certified Data Protection Expert – Loi 09-08.

Prérequis

Aucun prérequis formel n'est exigé.
Une connaissance de base en sécurité de l'information, gouvernance des données ou réglementation RGPD constitue un atout.

Durée

Cette formation dure 21 heures, réparties sur 3 parties.
À l'issue de la formation, un certificat de participation est délivré

Programme Détaille

Jour 1 (7 H)
• Présentation de la loi 09-08 et de ses textes d'application.
• Gouvernance d'un programme de protection de la vie privée
• Violation sur les données personnelles Consentement
• Analyse d'impact relative à la protection des données
Jour 2 (7 H)
• Principaux traitements de données soumis à une déclaration
• Principaux traitements de données soumis à une autorisation
• Transfert des données à l'international
Jour 3 (7 H)
• Mesures de sécurité
• Dispositif d'exercice des droits des personnes concernées
• Maintien du dispositif de conformité
Examen certifiant
(2 h – 100 QCM à livre fermé).



ISO 27701 FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la gestion d'un système de protection des données et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du PIMS dans le monde de l'entreprise. Au cours de cette formation, l'étudiant acquerra les bases de connaissances et certaines aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de la norme ISO 27701 pour la mise en œuvre et les opérations d'un PIMS. Sur base de cas d'exemples et d'exercices pratiques, l'étudiant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un PIMS en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles- ci dans une perspective de maîtrise des enjeux liés à la protection des données de leur organisation.

Public Cible

- Security Officers
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au SMSI dans une organisation
- Dirigeants d'une entreprise souhaitant sefamiliariser avec les aspects de Sécurité del'information
- Membres d'une équipe projet en sécurité de l'information
- Opérateurs en technologie de l'information
- Membres du personnel d'une organisation voulant se préparer pour un poste en sécurité de l'information

Objectifs

- Comprendre les enjeux du management d'un système de protection des données et sa mise en œuvre .
- Acquérir la terminologie et les connaissances de base nécessaires pour répondre aux exigences de l'ISO 27701.
- Découvrir les bonnes pratiques d'un système de protection des données selon l'ISO 27701.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 27701 Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Programme de gestion des risques selon la norme

- Le PIMS tel qu'exigé par la norme ISO 27701 - 7H
- Concepts de base liés à un système de Management de la protection des données
- Principes fondamentaux de la protection des données de la vie privée
- Principales clauses de l'ISO 27701
- Le contexte du PIMS au sein de l'entreprise et son champ d'application
- Aspects de leadership et engagement managérial
- Planification d'un PIMS
- Support des opérations d'un PIMS (documentation, ressources, etc.)

Fonctionnement du PIMS- 7H

- Détermination de l'impact sur la vie privée
- Déclaration d'applicabilité du PIMS
- Gestion de la documentation
- Sélection & mise en œuvre des mesures

Examen certifiant « PIMS Foundation »

1h, 50 questions QCM à livre fermé)



ISO 27701 LEAD IMPLEMENTER

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre de la gestion de la protection de la vie privée et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir l'intégrité du PIMS dans le respect des exigences de la norme ISO 27701 ainsi que le processus d'assurance qualité requis par les guides de pratiques associés. Sur base d'exemples réels et d'exercices concrets, l'étudiant sera amené durant la formation à mener à bien un projet d'implémentation de PIMS en développant des capacités en gestion de programmes et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées

Public Cible

- Directeurs intéressés par la gestion des données
- Consultants cherchant à maîtriser la mise en œuvre d'un système de management de la protection de la vie privée
- Responsables chargés de la protection des données à caractère personnel
- Conseillers experts en protection des données
- Experts techniques voulant se préparer pour un poste en protection des données de la vie privée
- Chargés de la conformité des lois

Objectifs

- Comprendre les principes de fonctionnement d'un PIMS selon l'ISO 27701
- Développer Les aptitudes nécessaires pour mener à bien un projet d'implémentation ISO 27701 dans le respect des exigences de la norme et les lignes directrices des normes ISO 27001 et ISO 27002.
- Acquérir la compétence de gestion d'une équipe projet pour lancer et maintenir un PIMS
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO27701
- Lead Implementer selon le niveau d'expérience.

Prérequis

Une connaissance de base de la protection des données est nécessaire pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).À l'issue de la formation, un certificat de participation est délivré

Programme Détaille

Le PIMS tel qu'exigé par la norme ISO/CEI 27701-7H

- PIMS – concepts de base
- Principes fondamentaux de la protection des données de la vie privée
- Les principales clauses de l'ISO 27701
- Le contexte du PIMS au sein de l'entreprise et son champ d'application
- Aspects de leadership et engagement managérial
- Planification d'un PIMS
- Politique de protection de la vie privée.

Planification de la mise en œuvre d'un PIMS - 7H

- Détermination de l'impact sur la vie privée déclaration d'applicabilité du PIMS
- Gestion de la documentation
- Sélection des mesures
- Mise en œuvre des mesures

Examen certifiant « ISO27701 Foundation »

1h, 50 questions QCM à livre fermé)

Mettre en œuvre un PIMS – 7H

- Mise en œuvre des mesures d'un PIMS • Mise en œuvre des mesures pour les contrôleurs
- Mise en œuvre des mesures pour les processeurs • Améliorer et préparer le PIMS à une certification-7H évaluation du PIMS
- Amélioration continue du PIMS • Comment préparer le système à un audit interne ?
- Traitement des non conformités • Comment préparer le système à un audit de certification ?

Clôture et suivi d'un PIMS-7H

- Exercices préparatoires supplémentaires
- Présentation des conclusions
- Présentation et utilisation des outils de suivi du cycle de vie du PIMS
- Clôture de la formation

Examen certifiant « ISO 27701 Practitioner »

2 heures , 100 questions QCM à livre fermé.

Les organisations sont aujourd'hui confrontées à des risques susceptibles d'affecter leurs activités à tout moment.
La continuité d'activité permet d'anticiper ces événements, d'en limiter les conséquences et d'assurer une reprise rapide des activités critiques. Développer les compétences dans ce domaine est essentiel pour renforcer la résilience et la pérennité des organisations.



ISO 22301 FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la gestion de la continuité d'activité et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du SMCA dans le monde de l'entreprise. Au cours de cette formation, l'étudiant acquerra les bases de connaissances et certaines aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de la norme ISO 22301 pour la mise en œuvre et les opérations d'un SMCA. Sur base de cas d'exemples et d'exercices pratiques, participant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un SMCA en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles- ci dans une perspective de maîtrise des enjeux liés à la continuité d'activité au sein de leur organisation

Public Cible

- Business Continuity Managers
- Responsables ou collaborateurs des services généraux d'une entreprise
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au SMCA dans une organisation
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de continuité d'activité
- Membres d'une équipe projet en continuité d'activité
- Opérateurs en technologie de l'information
- Membre du personnel d'une organisation voulant se préparer pour un poste en continuité d'activité

Objectifs

- Comprendre les enjeux du management de la continuité d'activité et sa mise en œuvre.
- Acquérir la terminologie et les connaissances de base nécessaires pour répondre aux exigences de l'ISO 22301 dans le contexte d'une entreprise
- Découvrir les bonnes pratiques de management de la sécurité de l'information et son articulation avec la gestion des risques
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified BCMS Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Le SMCA tel qu'exigé par la norme ISO 22301 : 2019 – 7H

- Système de Management de la Continuité d'Activité – concepts de base
- Principes fondamentaux de la continuité d'activité
- Les clauses 4 à 10 de l'ISO 22301 et les lignes directrices de l'ISO 22313
- Le contexte du SMCA au sein de l'entreprise et son champ d'application
- Aspects de leadership et engagement managérial
- Planification d'un SMCA (bilan d'impact sur les activités, mesures applicables, etc.)
- Support des opérations d'un SMCA (documentation, ressources, etc.)

Fonctionnement du SMCA– 7H

- Gestion des opérations d'un SMCA
- Surveillance du SMCA (journalisation, audit et revue de direction)
- Évaluation de l'efficacité des opérations et gestion des métriques
- Actions correctives et amélioration continue
- Processus de certification ISO 22301
- Présentation de la documentation nécessaire aux opérations du SMCA (toolbox)

Examen certifiant « BCMS Foundation »

- 1h, 50 questions QCM à livre fermé



ISO 22301 LEAD IMPLEMENTER

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre de la gestion de la continuité d'activité et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, l'étudiant acquerra les bases de connaissance et lesaptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir l'intégrité du SMCA dans le respect des exigences de la norme ISO 22301 ainsi que le processus d'assurance qualité requis par les guides de pratiques associés. Sur base d'exemples réels et d'exercices concrets, participant sera amené durant la formation à mener à bien un projet d'implémentation de SMCA en développant des capacités en gestion de programmes et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Business Continuity Managers
- Opérateurs de tests en continuité
- Responsables services généraux en entreprise
- Chefs de projet ou consultants souhaitant maîtriser la mise en œuvre d'un système de management de la Continuité d'Activité
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques opérationnels
- Membres d'une équipe de continuité d'activité
- Conseillers experts en continuité d'activité
- Experts techniques se préparant à un poste en continuité d'activité

Objectifs

- Comprendre les principes de fonctionnement d'un SMCA selon ISO 22301
- Développer les aptitudes nécessaires pour mener à bien un projet d'implémentation ISO 22301 dans le respect des exigences de la norme et les lignes directrices des normes ISO 22313, 22316, 27031et 24762
- Acquérir la compétence de gestion d'une équipe projet pour lancer et maintenir un SMCA
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified BCMS Lead Implementer selon le niveau d'expérience.

Prérequis

Une connaissance de base de la continuité d'activité et de la norme ISO 22301 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le SMCA tel qu'exigé par la norme ISO 22301 : 2019 - 7H
Pour plus d'information voir le programme détaillé de la formation BCMS Foundation.
Fonctionnement du SMCA - 7H
Pour plus d'information voir le programme détaillé de la formation BCMS Foundation.
Examen certifiant « BCMS Foundation (ISO 22301) »
1h, 50 questions QCM à livre fermé
Préparation et démarrage d'un projet SMCA – 7H
- Planification d'un projet SMCA
- Périmètre du projet et définition du champ d'application du SMCA
- Les acteurs du projet – Rôles et responsabilités des parties prenantes
- Business Case et méthodologie de gestion de projet
- Obtenir le soutien des parties prenantes et de la direction
- Gestion des relations avec les parties intéressées durant le projet d'implémentation
- Documentation du SMCA, politiques et procédures du SMCA – Les différents plans de continuité
- Bilan d'impact sur les activités et gestion des risques opérationnels
- Présentation et utilisation des outils de préparation au projet et BIA (via étude de cas)

Les opérations et la performance d'un SMCA-7H
- Stratégies de Continuité d'Activité • Communication, sensibilisation et formation
- Gestion des incidents majeurs et des interruptions de la continuité opérationnelle
- Mesures de protection et d'atténuation des impacts • Crises & gestion de l'urgence
- Les différents composants du plan de continuité d'activité
- Surveillance, mesure, analyse et évaluation du SMCA
- Présentation et utilisation des outils de réalisation et de suivi des plans (via étude de cas)

Cycle de vie et pérennité du SMCA-7H
- Audit interne du SMCA, gestion de la conformité
- Revue de direction • Gestion de l'amélioration continue et plans d'actions
- Présentation et utilisation des outils de suivi du cycle de vie du SMCA (via étude de cas)

Examen certifiant « BCMS Practitioner »
2h,100 questions QCM à livre fermé



ISO 22301 LEAD AUDITOR

Cette formation de 35 heures offre aux participantsl'occasion de monter en compétence sur la fonction d'assurance de la gestion de la continuité d'activité et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser divers types d'audits de 1e, 2e ou 3e partie dans le respect des exigences de la norme ISO 19011 ainsi que le processus de certification requis par la norme ISO 17021. Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, l'étudiant sera amené durant la formation à mener à bien un audit de SMCA en développant des capacités en gestion de programmes et de techniques d'audit ainsi qu'en gestion d'équipe, à travers la communication avec le client d'audit.

Public Cible

- Auditeurs internes
- Auditeurs cherchant à réaliser et à mener des audits dans les systèmes de sécurité d'informations
- Gestionnaires de projets ou consultants souhaitant maîtriser les audits des systèmes de continuité d'activité
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de continuité d'activité
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en continuité d'activité

Objectifs

- Comprendre les principes de fonctionnement d'un SMCA selon ISO 22301
- Développer les aptitudes nécessaires pour mener à bien un audit ISO 22301 dans le respect des exigences de l'ISO 19011 et les spécifications de l'ISO 17021.
- Acquérir la compétence de gestion d'une équipe d'auditeurs de SMCA
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified BCMS Lead
- Auditor selon le niveau d'expérience.

Prérequis

Une connaissance de base de la continuité d'activité et de la norme ISO 22301 est nécessaire

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le SMCA tel qu'exigé par la norme ISO 22301 : 2019-7H
Pour plus d'information voir le programme détaillé de la formation BCMS Foundation.
Fonctionnement du SMCA-7H
Pour plus d'information voir le programme détaillé de la formation BCMS Foundation.
Examen certifiant « BCMS Foundation (ISO 22301) »
1h, 50 questions QCM à livre fermé
Préparation et démarrage de l'audit d'un SMCA-7H
- Concepts de base, principes et critères d'audit selon ISO 19011
- Déroulement général d'un audit de SMCA
- Audits interne et externe ü Les acteurs de l'audit
- Planification et mise en œuvre d'un programme d'audit
- Activités préparatoires à l'audit • Gestion des relations avec l'audité avant et pendant l'audit
- Documentation de l'audit • Audit documentaire (audit d'étape 1)
- Présentation et utilisation des outils de préparation à un audit (via étude de cas)

Réalisation de l'audit sur site d'un SMCA-7H
- Préparation de l'audit sur site (audit d'étape 2)
- Approche d'audit fondée sur la preuve et les risques
- Les différentes procédures d'audit • Création de plans de test d'audit
- Exercices pratiques : simulations d'entretiens et de collecte de preuve
- Aspects liés aux rapports d'audit • Revue de qualité des constats d'audit et préparation des conclusions
- Présentation et utilisation des outils de réalisation d'un audit (via étude de cas)

Clôture et suivi de l'audit - 7H
- Présentation des conclusions • Réunion de clôture
- Rédaction du rapport d'audit • Suites à l'audit du SMCA (plans d'action et suivi de ceux-ci)
- Audits de surveillance et de suivi
- Présentation et utilisation des outils de reporting d'un audit (via étude de cas pratique)

Examen certifiant « BCMS Auditor »
- 2h ,100 questions QCM à livre fermé

Qualité, Santé, Sécurité

Qualité

La qualité est un levier stratégique pour améliorer la performance, renforcer la satisfaction des clients et favoriser l'amélioration continue. La mise en place d'un système de management de la qualité permet d'optimiser les processus, de maîtriser les risques et de répondre aux exigences des parties prenantes. Développer les compétences dans ce domaine contribue à accroître l'efficacité des organisations et à renforcer leur compétitivité.

Santé & Sécurité au travail

Préserver la santé et la sécurité des collaborateurs est une priorité pour toute organisation. La mise en œuvre d'un système de management de la santé et de la sécurité au travail permet de prévenir les risques professionnels, d'améliorer les conditions de travail et de favoriser une culture de prévention. Développer les compétences dans ce domaine contribue à protéger les collaborateurs, à renforcer la conformité réglementaire et à améliorer la performance durable de l'organisation.



ISO 9001 FOUNDATION

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de gestion de la qualité et de se familiariser avec les principes, méthodes et procédures appliquées au sujet du mangement de la qualité dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les connaissances de base et les aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de la norme ISO 9001 pour la mise en œuvre d'une stratégie de management s'un SMQ. Sur la base de cas d'exemples et d'exercices pratiques, l'étudiant sera amené durant la formation à mieux cerner les aspects de mise en œuvre d'un système de management de la qualité, en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles-ci dans le contexte d'une entreprise.

Public Cible

- Spécialistes en management de la qualité
- Responsables de la qualité
- Directeurs de la qualité
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au management d'un SMQ
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects relatifs à la qualité
- Membres du personnel d'une organisation voulant se préparer pour un poste en gestion de la qualité

Objectifs

- Comprendre les enjeux du management de la qualité
- Acquérir la terminologie et les connaissances nécessaires pour répondre aux exigences de
- l'ISO 9001 dans le contexte d'une entreprise
- Découvrir les bonnes pratiques de gestion d'un Système de management de la qualité
- Réussir l'examen de CERTI-TRUST™

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à la formation conduisant à cette certification.

Durée

14 heures, réparties sur 2 parties.
À l'issue de la formation, une attestation de participation à la formation sera remis aux participants

Programme Détaille

Introduction à la norme ISO 9001- 7H
- Généralités
- Terminologie
- le Système de Management de la Qualité (SMQ) tel qu'exigé par la norme ISO 9001: 2015

Fonctionnement du Système de Management de la Qualité- 7H
- Fonctionnement du SMQ
- Outils de gestion du cycle de vie d'un SMQ
- Exercices et ateliers

Examen ISO 9001 Foundation
- (1 heure-50questions QCM)



ISO 9001 LEAD AUDITOR

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction d'assurance de la gestion de la qualité et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser divers types d'audits de 1e, 2e ou 3e partie dans le respect des exigences de la norme ISO 19011. Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, participant sera amené durant la formation à mener à bien un audit de SMQ en développant des capacités en gestion de programmes et de techniques d'audit ainsi qu'en gestion d'équipe.

Public Cible

- Spécialistes en management de la qualité
- Responsables de la qualité
- Directeurs du département qualité
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au management d'un SMQ
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects relatifs à la qualité
- Membres du personnel d'une organisation voulant se préparer pour un poste en gestion de la qualité

Objectifs

- Comprendre les principes de fonctionnement d'un SMQ selon l'ISO 9001
- Développer les aptitudes nécessaires pour mener à bien un audit SMQ dans le respect des exigences de l'ISO 19011.
- Acquérir la compétence de gestion d'une équipe d'auditeurs de SMQ
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified SMQ Lead Auditor selon le niveau d'expérience

Prérequis

Une connaissance de base du management de la qualité est nécessaire pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits). CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Introduction à la norme ISO 9001- 7H

• Généralités • Terminologie • Le Système de Management de la Qualité (SMQ) tel qu'exigé par la norme ISO 9001: 2015

Fonctionnement du Système de Management de la Qualité- 7H

• Fonctionnement du SMQ
• Outils de gestion du cycle de vie d'un SMQ
• Exercices et ateliers

Examen ISO 9001 Foundation

• (1 heure-50 questions QCM)

Préparation et démarrage de l'audit d'un SMQ - 7H

• Concepts de base, principes et critères d'audit selon ISO 19011
• Déroulement général d'un audit de SMQ
• Audits interne et externe • Les acteurs de l'audit
• Planification et mise en œuvre d'un programme d'audit
• Activités préparatoires à l'audit
• Gestion des relations avec l'audité avant et pendant l'audit
• Documentation de l'audit
• Audit documentaire (audit d'étape 1)
• Présentation et utilisation des outils de préparation à un audit (via étude de cas)

Réalisation de l'audit sur site d'un SMQ - 7H

• Préparation de l'audit sur site (audit d'étape 2)
• Approche d'audit fondée sur la preuve et les risques
• Les différentes procédures d'audit
• Création de plans de test d'audit
• Exercices pratiques : simulations d'entretiens et de collecte de preuve
• Aspects liés aux rapports d'audit
• Revue de qualité des constats d'audit et préparation des conclusions
• Présentation et utilisation des outils de réalisation d'un audit (via étude de cas)

Clôture et suivi de l'audit - 7H

• Présentation des conclusions
• Réunion de clôture • Rédaction du rapport d'audit
• Suites à l'audit du SMQ • Audits de surveillance et de suivi
• Présentation et utilisation des outils de reporting d'un audit
• Étude de cas pratique
• Examen certifiant « ISO 9001 Auditor »



ISO 9001 LEAD IMPLEMENTER

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre du management de la qualité selon l'ISO 9001 et de se préparer par la pratique à diriger des équipes, sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, le participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer etgarantir la conformité, l'efficacité et la performance d'un SMQ dans le respect des exigences de la norme ISO 9001 ainsi que les guides de bonnes pratiques associés. Sur base d'exemples réels et d'exercices concrets, le participant sera amené durant la formation à mener à bien un projet d'implémentation de SMQ en développant des capacités en gestion de programmes et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Spécialistes en management de la qualité
- Responsables de la qualité
- Directeurs du département qualité
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au management d'un SMQ
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects relatifs à la qualité
- Membres du personnel d'une organisation voulant se préparer pour un poste en gestion de la qualité

Objectifs

- Acquérir une compréhension globale des concepts, des approches, des méthodes, des techniques et des étapes de mise en œuvre d'un SMQ selon l'ISO9001
- Comprendre les enjeux, les exigences des parties intéressées, les exigences réglementaires et les exigences des normes ISO 9001
- Savoir gérer une équipe SMQ
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified SMQ lead Implementer, selon le niveau d'expérience.

Prérequis

Une connaissance de base du management de la qualité est nécessaire pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits)
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Introduction à la norme ISO 9001- 7H

• Généralités
• Terminologie
• le Système de Management de la Qualité (SMQ) tel qu'exigé par la norme ISO 9001: 2015

Fonctionnement du Système de Management de la Qualité-7H

• Fonctionnement du SMQ
• Outils de gestion du cycle de vie d'un SMQ
• Exercices et ateliers

Examen ISO 9001 Foundation (1heure-50 questions QCM)

Le fonctionnement d'un SMQ tel qu'exigé par la norme ISO 9001-7h

• Etat des lieux
• Organisation du projet SMQ
• Comprendre l'organisation
• Référentiel documentaire du SMQ

La mise en œuvre d'un projet SMQ-7h

• Gestion et traitement des risques
• Définir et mettre à jour les processus de management de la qualité
• Formation, sensibilisation et communication
• Maitrise opérationnelle

L'évaluation de la performance du SMQ et l'audit interne-7h évaluation de la performance

• Audit interne et revue de direction
• Amélioration continue
• Transfert aux opérations
• Processus de certification

Examen certifiant « SMQ Practitioner»

2h ,100 questions QCM à livre fermé



ISO 19011 AUDITEUR INTERNE

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la fonction de l'audit interne et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser un audit interne dans le respect des exigences de la norme ISO 19011. Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, l'apprenant sera amené durant la formation à mener à bien un audit interne en développant des capacités en gestion de programmes et de techniques d'audit ains qu'en gestion d'équipe d'auditeurs internes.

Public Cible

- Auditeurs internes
- Spécialistes en audit
- Chefs de projet d'audit
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de l'audit interne
- Membres d'une équipe d'auditeurs
- Membre du personnel d'une organisation voulant se préparer pour un poste en audit interne

Objectifs

- Comprendre les principes de fonctionnement d'un processus d'audit selon ISO 19011
- Développer les aptitudes nécessaires pour mener à bien un audit interne selon les exigences de la norme ISO 19011
- Acquérir la compétence de gestion d'une équipe d'auditeurs internes
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de ISO 19011 Auditeur interne certifié.

Prérequis

La connaissance des bases en Audit des systèmes de management est requise pour participer à cette formation.

Durée

21 heures, réparties sur 3 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 21 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Les principes fondamentaux de l'audit-7H
- Généralités
- Fondamentaux de l'audit
- Déontologie et respect des principes
- Approche d'audit fondée sur la preuve et le risque

Réalisation de l'audit interne-7H
- Déclenchement d'un audit
- Préparation de l'audit
- Démarrage de l'audit sur site
- Bonnes pratiques durant
- Les audits les procédures d'audit
- Recueil et vérification des informations obtenues durant l'audit
- Rédaction des constats et rapports de non conformité

Clôture et suivi de l'audit-7H
- Clôture d'un audit interne
- Activités de suivi
- Compétences et évaluation des auditeurs
- Clôture de la formation

Examen ISO 19011 Auditeur Interne Certifié
(2h-100 questions QCM)



ISO 45001 FOUNDATION

Cette une formation de 14 heures (réparties sur 2 jours) permet au participant de découvrir les fondamentaux du management de de la Santé et de la Sécurité au Travail, les concepts de base, et de comprendre un projet de mise en œuvre d'un SMSST. Au cours de cette formation l'apprenant acquerra la terminologie et les connaissances de base nécessaires sur la base des exigences de l'ISO 45001, au sein d'une organisation.
Durant cette formation, participant acquerra les connaissances et les capacités de planifier, mettre en œuvre, évaluer et garantir l'intégrité d'un SMSST conformément aux exigences de la norme ISO 45001, dans le contexte d'une entreprise.

Public Cible

- les spécialistes en gestion de la Santé et de la Sécurité au Travail
- Toute personne intéressée par le domaine de la gestion de la SST
- Chefs de projets ou consultants souhaitant accompagner une organisation dans la mise en œuvre d'un système de management de la Santé et de la Sécurité au Travail selon l'ISO 45001
- Les auditeurs qui souhaitent comprendre pleinement le processus de mise en œuvre d'un SME et bonnes pratiques associées.
- Médecins, Responsables en entreprise souhaitant renforcer leurs compétences en management la Santé et de la Sécurité au Travail

Objectifs

- Comprendre les questions de gestion d'un SMSST et sa mise en œuvre
- Acquérir les connaissances de base pour remplir les exigences de l'ISO 45001 dans le contexte d'une organisation
- Découvrir les bonnes pratiques de gestion d'un SMSST selon l'ISO 45001.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 45001 Foundation

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

Cette formation dure 14 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).

Programme Détaille

Introduction - 7 heures
- Introduction à la formation et aux normes
- Terminologie
- Le Système de Management de la Santé et de la Sécurité au Travail tel qu'exigé par la norme ISO 45001: 2018

Fonctionnement du SMSST - 7 heures
- Le fonctionnement d'un système de Management de la
- Santé et de la Sécurité au Travail
- Outils de gestion du cycle de vie d'un SMSST
- Exercices
- Ateliers

Examen certifiant « ISO 45001 Foundation »
1h, 50 questions QCM à livre fermé)



ISO 45001 LEAD IMPLEMENTER

Cette formation offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre du management de la Santé et de la Sécurité au Travail (5SMSST) selon l'ISO 45001 et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, le participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir la conformité, l'efficacité et la performance d'un SMSST dans le respect des exigences de la norme ISO 45001 ainsi que les guides de bonnes pratiques associés. Sur base d'exemples réels et d'exercices concrets, le participant sera amené durant la formation à mener à bien un projet d'implémentation de SMSST en développant des capacités en gestion de programme et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers lacommunication avec les différentes parties intéressées.

Public Cible

- Chefs de projets ou consultants souhaitant accompagner une organisation dans la mise en œuvre d'un système de management de la Santé et de la Sécurité au Travail selon l'ISO 45001
- Les auditeurs qui souhaitent comprendre pleinement le processus de mise en œuvre d'un SMSST et bonnes pratiques associées.
- Médecins, Responsables en entreprise souhaitant renforcer leurs compétences en management la Santé et de la Sécurité au Travail

Objectifs

- Acquérir une compréhension globale des concepts, des approches, des méthodes, des techniques et des étapes de mise en œuvre d'un SMSST selon l'ISO45001
- Comprendre les enjeux, les exigences des parties intéressées, les exigences réglementaires et les exigences des normes ISO 45001
- Savoir gérer une équipe SST
- Solliciter la qualification de Certified Lead implementer selon le niveau d'expérience

Prérequis

Une connaissance de base des normes de système de management ainsi qu'une expérience dans l'audit et/ou la mise en œuvre de ces systèmes est recommandée pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Introduction - 7 heures
- Introduction à la formation et aux normes
- Terminologie
- Le Système de Management de la Santé et de la Sécurité au Travail tel qu'exigé par la norme ISO 45001: 2018

Fonctionnement du SMSST - 7 heures
- Le fonctionnement d'un système de
- Management de la Santé et de la Sécurité au Travail
- Outils de gestion du cycle de vie d'un SMSST
- Exercices
- Ateliers

Examen certifiant « ISO 45001 Foundation »
1h, 50 questions QCM à livre fermé)

Analyse de contexte-7 heures
- Analyse de contexte
- Définition du domaine d'application
- Planification du projet
- Conception de la structure organisationnelle
- Documentaire du SMSST
- Exercices
- Ateliers

Analyse des risques-7 heures
- Analyse des risques,
- Définition des objectifs,
- Définition du système documentaire du SMSST formation, sensibilisation et communication
- Etude de cas

Maitrise opérationnelle, surveillance, mesure, analyse et évaluation – 7H
- Maitrise opérationnelle, surveillance, mesure, analyse et évaluation des performances.
- Audits internes, revue de direction et amélioration du SMSST
- Exercices et ateliers (QCM, questions ouvertes, mini cas)
- Clôture de la formation

Examen certifiant « ISO 45001 Practitioner »
2 heures , 100 questions QCM à livre fermé.



ISO 45001 LEAD AUDITOR

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction d'assurance de la gestion d'un système de Management de la Santé et de la Sécurité au Travail tel qu'exigé par la norme ISO 45001: 2018 et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser divers types d'audits de 1e, 2e ou 3e partie dans le respect des exigences de la norme ISO 19011. Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, participant sera amené durant la formation à mener à bien un audit de SMSST en développant des capacités en gestion de programmes et de techniques d'audit ainsi qu'en gestion d'équipe, à travers la communication avec le client d'audit.

Public Cible

- Auditeurs cherchant à réaliser des audits SMSST
- Chefs de projets ou consultants souhaitant s'initier à /ou réaliser un audit d'un système de management de la Santé et de la Sécurité au Travail selon l'ISO 45001
- Les auditeurs qui souhaitent comprendre pleinement le processus de mise en œuvre d'un SME et bonnes pratiques associées.
- Responsables en entreprise souhaitant renforcer leurs compétences en audit d'un système de management de la Santé et de la Sécurité au Travail

Objectifs

- Comprendre les concepts, les approches, les méthodes, les techniques et les étapes de mise en œuvre d'un SMSST selon l'ISO45001
- Planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Comprendre les enjeux, les exigences des parties intéressées, les exigences réglementaires et les exigences des normes ISO 45001
- Savoir gérer une équipe d'audit SMSST
- Solliciter la qualification de Certified Lead Auditor selon le niveau d'expérience.

Prérequis

Une connaissance de base des normes de systèmebde management ainsi qu'une expérience dansbl'audit et/ou la mise en œuvre de ces systèmes estbrecommandée pour participer à ce cours.

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Introduction - 7 heures
- Introduction à la formation et aux normes
- Terminologie
- Le Système de Management de la Santé et de la Sécurité au Travail tel qu'exigé par la norme ISO 45001: 2018

Fonctionnement du SMSST - 7 heures
- Le fonctionnement d'un système de
- Management de la Santé et de la Sécurité au Travail
- Outils de gestion du cycle de vie d'un SMSST
- Exercices
- Ateliers

Examen certifiant « ISO 45001 Foundation »
1h, 50 questions QCM à livre fermé)

Étape 1 : Audit d'un Système de Management de la Santé et de la Sécurité au Travail tel qu'exigé par la norme ISO 45001: 2018 – 7 heures
- Concepts fondamentaux d'audit
- Approche d'audit fondée sur les preuves
- Commencement de l'audit
- 1ère étape de l'audit

Étape 2 : Audit d'un SMSST - 7 heures
- 2ème Étape de l'audit
- Procédures d'audit
- Rédaction des plans de tests
- Rédaction des constats d'audit
- Rédaction des rapports de non-conformités
- Exercices & ateliers (QCM, questions ouvertes, mini cas)

Clôture de l'audit d'un SMSST - 7 heures
- Clôture de l'audit
- évaluation et contrôle
- Clôture de la formation

Examen certifiant « ISO 45001 Auditor»
2 heures , 100 questions QCM à livre fermé.

Environnement, ESG, Développement durable

Environnement

La protection de l'environnement est devenue un enjeu stratégique pour les organisations. La mise en place d'un système de management environnemental permet de maîtriser les impacts environnementaux, d'améliorer les performances et de répondre aux exigences réglementaires. Développer les compétences dans ce domaine favorise une démarche responsable et durable.

ESG & Développement durable

Préserver la santé et la sécurité des collaborateurs est une priorité pour Les enjeux environnementaux, sociaux et de gouvernance (ESG) occupent une place croissante dans la stratégie des organisations. Développer les compétences dans ce domaine permet d'intégrer les principes du développement durable, de répondre aux attentes des parties prenantes et de créer une valeur durable.



ISO 14001 FOUNDATION

Cette formation de 14 heures (réparties sur 2 jours) offre aux participants l'occasion de monter en compétences sur les aspects principaux de la gestion d'un système de management de l'environnement, de se familiariser avec les principes d'un SME dans le monde de l'entreprise. Au cours de cette formation, le participant acquerra les connaissances de base et certaines aptitudes lui permettant de comprendre la structure de la norme ISO 14001 et les fondements d'une démarche de gestion environnementale, sur la base de cas d'exemples et d'exercices pratiques.

Public Cible

- Toute personne intéressée par la gestion de l'environnement.
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés à la gestion de l'environnement.
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la gestion de l'environnement.
- Membres d'une équipe projet en management de l'environnement.
- Membres du personnel d'une organisation voulant se préparer pour un poste en gestion de l'environnement.
- Responsables en entreprise souhaitant renforcer leurs compétences en management de l'environnement

Objectifs

- Maitriser les principes de la gestion de l'environnement
- Comprendre le fonctionnement d'un système de management de l'environnement
- Acquérir la compétence à structurer et mettre en œuvre un SME sur la base de l'ISO 14001
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO14001 Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Introduction à la formation - 7H
- Généralités
- Contexte & Historique
- Terminologie
- Le Système de Management de l'Environnement (SME) tel qu'exigé par la norme ISO 14001: 2015

Fonctionnement d›un SME sur la base de la norme
- ISO 14001-7H
- Un cadre normatif largement reconnu : ISO 14001
- Fonctionnement du SME
- Outils de gestion du cycle de vie d'un SME

Exercices et ateliers
Examen certifiant « ISO 14001 Foundation »
1h, 50 questions QCM à livre fermé



ISO 14001 LEAD AUDITOR

Cette formation de 35 heures offre aux participants l'occasion de monter en compétence sur la fonction d'assurance de la gestion de l'environn ment et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement a pliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier et réaliser divers types d'audits de 1e, 2e ou 3e partie dans le respect des exigences de la norme ISO 19011. Sur base de cas d'exemples réels issus du terrain et d'exercices concrets, participant sera amené durant la formation à mener à bien un audit de SME en développant des capacités en gestion de programmes et de techniques d'audit ainsi qu'en gestion d'équipe.

Public Cible

- Toute personne intéressée par la gestion de l'environnement.
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés à la gestion de l'environnement.
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la gestion de l'environnement.
- Membres d'une équipe projet en management de l'environnement.
- Membres du personnel d'une organisation voulant se préparer pour un poste en gestion de l'environnement.
- Responsables en entreprise souhaitant renforcer leurs compétences en management de l'environnement

Objectifs

- Comprendre les principes de fonctionnement d'un SME selon ISO 14001
- Développer les aptitudes nécessaires pour mener à bien un audit ISO 14001 dans le respect des exigences de l'ISO 19011.
- Acquérir la compétence de gestion d'une équipe d'auditeurs de SME
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified SME Lead Auditor selon le niveau d'expérience.

Prérequis

Une connaissance de base de la gestion de l'environnement et de la norme ISO 14001 est nécessaire pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Introduction à la formation
- Généralités
- Le SME tel qu'exigé par la norme ISO 14001: 2015

Fonctionnement d'un SME sur la base de la norme ISO 14001
- Un cadre normatif largement reconnu: ISO 14001
- Fonctionnement du SME
- Outils de gestion du cycle de vie d'un SME

Examen certifiant « ISO 14001 Foundation »
1h, 50 questions QCM à livre fermé

Réparation et démarrage de l'audit d'un SME -7H
- Concepts de base, principes et critères d'audit selon ISO 19011
- Déroulement général d'un audit de SME
- Audits interne et externe • Les acteurs de l'audit
- Planification et mise en œuvre d'un programme d'audit
- Activités préparatoires à l'audit
- Gestion des relations avec l'audité avant et pendant l'audit
- Documentation de l'audit
- Audit documentaire (audit d'étape 1)
- Présentation et utilisation des outils de préparation à un audit (via étude de cas)

Réalisation de l'audit sur site d'un SME - 7H
- Préparation de l'audit sur site (audit d'étape 2)
- Approche d'audit fondée sur la preuve et les risques
- Les différentes procédures d'audit
- Création de plans de test d'audit
- Exercices pratiques : simulations d'entretiens et de collecte de preuve
- Aspects liés aux rapports d'audit
- Revue de qualité des constats d'audit et préparation des conclusions
- Présentation et utilisation des outils de réalisation d'un audit (via étude de cas)

Clôture et suivi de l'audit-7H
- Présentation des conclusions • Réunion de clôture
- Rédaction du rapport d'audit • Suites à l'audit du SME
- Audits de surveillance et de suivi
- Présentation et utilisation des outils de reporting d'un audit étude de cas pratique

Examen certifiant « ISO 14001 Auditor »
2h ,100 questions QCM à livre fermé



ISO 14001 LEAD IMPLEMENTER

Cette formation offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre du management de l'environnement selon l'ISO 14001 et de se préparer par la pratique à gérer des équipes opérationnelles sur la base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise appliquées dans le monde de l'entreprise. Au cours de cette formation, le participant acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir la conformité, l'efficacité et la performance d'un SME dans le respect des exigences de la norme ISO 14001 ainsi que les guides de bonnes pratiques associés. Sur base d'exemples réels et d'exercices concrets, le participant sera amené durant la formation à mener à bien un projet d'i plémentation de SME en développant des capacités en gestion de programme et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Toute personne intéressée par la gestion de l'environnement.
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés à la gestion de l'environnement.
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la gestion de l'environnement.
- Membres d'une équipe projet en management de l'environnement.
- Responsables voulant se préparer pour un poste en gestion de l'environnement.

Objectifs

- Acquérir une compréhension globale des concepts, des approches, des méthodes, des techniques et des étapes de mise en œuvre d'un SME selon l'ISO 14001
- Comprendre les enjeux, les exigences des parties intéressées, les exigences réglementaires et les exigences des normes ISO 14001
- Savoir gérer une équipe SME
- Solliciter la qualification de Certified ISO 14001 Lead Implementer, selon le niveau d'expérience.

Prérequis

Une connaissance de base de la gestion de l'environnement et de la norme ISO 14001 est nécessaire pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Introduction à la formation - 7H
- Contexte & Historique
- Terminologie
- Le Système de Management de l'Environnement (SME) tel qu'exigé par la norme ISO 14001: 2015

Fonctionnement d'un SME sur la base de la norme ISO 14001- 7H
- Un cadre normatif largement reconnu : ISO 14001
- Outils de gestion du cycle de vie d'un SME
- Exercices et ateliers

Examen certifiant « ISO 14001 Foundation »
1h, 50 questions QCM à livre fermé

Analyse de contexte – 7H
- Analyse de contexte
- Définition du domaine d'application
- Planification du projet
- Conception de la structure organisationnelle
- Documentaire du SME
- Exercices
- Ateliers

Analyse des risques – 7H
- Analyse des risques,
- Définition des objectifs,
- Définition du système documentaire du SME
- Formation, sensibilisation et communication
- Etude de cas (Mise en œuvre d›un SME)

Maitrise opérationnelle, surveillance, mesure, analyse et évaluation – 7H
- Maitrise opérationnelle, surveillance, mesure, analyse et évaluation des performances.
- Audits internes, revue de direction et amélioration du SME
- Exercices et ateliers (QCM, questions ouvertes)
- Clôture de la formation

Examen certifiant « SME Practitioner»
2h ,100 questions QCM à livre ferméF



ISO 26000 FOUNDATION

Cette formation de 14 heures (réparties sur 2 jours) offre aux participants l'occasion de monter en compétences sur les aspects principaux de la responsabilité sociétale des entreprises et du développement durable, de se familiariser avec les principes de la RSE et du DD dans le monde de l'entreprise. Au cours de cette formation, le participant acquerra les connaissances de base et certaines aptitudes lui permettant de comprendre la structure de la norme ISO 26000 et les fondements d'une démarche RSE, sur la base de cas d'exemples et d'exercices pratiques.

Public Cible

- Toute personne intéressée par la RSE et le DD.
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés à la RSE et au DD dans une organisation .
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la RSE.
- Membres d'une équipe projet en développement durable.
- Membres du personnel d'une organisation voulant se préparer pour un poste en RSE ou en DD.
- Les spécialistes en RSE et en DD.

Objectifs

- Maitriser les principes de la RSE et du DD
- Comprendre le fonctionnement d'une démarche RSE selon ISO26000
- Acquérir la compétence à structurer et mettre en œuvre un projet RSE sur la base de l'ISO 26000
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO26000 Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à la formation conduisant à cette certification.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Les fondamentaux de la RSE sur la base de la norme ISO 26000 - 7H
- Généralités
- Contexte & Historique de l'émergence de la RSE
- Concepts de la RSE et Tendances Initiatives Nationales (Ex: Maroc)
- Pourquoi une démarche RSE en entreprise?

Introduction à la norme ISO 26000 - 7H
- Un cadre normatif largement reconnu : ISO 26000
- ISO 26000 : Détail des questions centrales

Examen certifiant « ISO 26000 Foundation »
1h, 50 questions QCM à livre fermé



ISO 26000 LEAD IMPLEMENTER

Cette formation de 35 heures (réparties sur 5 jours) fournit aux participants l'occasion de découvrir l'approche de la mise en œuvre d'une démarche RSE, d'en évaluer la performance en s'appuyant sur les bonnes pratiques de la norme ISO 26000. Pendant cette formation, le participant acquerra les connaissances et les capacités nécessaires pour mener à bien un projet de mise en œuvre d'une démarche RSE, d'analyse de la matérialité et de reporting RSE ou ESG. La formation s'appuie sur une étude de cas et desoutils méthodologiques, et donne le droit à la certification ISO 26000 Lead Implementer.

Public Cible

- les spécialistes en RSE et en DD
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés à la RSE et au DD dans une organisation .
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la RSE.
- Membres d'une équipe projet en développement durable.
- Membres du personnel d'une organisation voulant se préparer pour un poste en RSE ou en DD.

Objectifs

- Comprendre les principes de la RSE et du DD et le fonctionnement d'une démarche RSE selon ISO26000.
- Développer les aptitudes nécessaires pour conseiller une entreprise pour intégrer une stratégie RSE sur la base de la norme ISO 26000.
- Acquérir la compétence à structurer et mettre en œuvre un projet RSE sur la base de l'ISO 26000.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO26000 Lead Implementer.

Prérequis

Une connaissance de base de la RSE et une certification ISO 26000 Foundation sont nécessaires pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Les fondamentaux de la RSE sur la base de la norme ISO26000-7H
- Contexte & Historique de l'émergence de la RSE
- Concepts de la RSE et Tendances
- Initiatives Nationales (Ex: Maroc)
- Pourquoi une démarche RSE en entreprise?

Introduction à la norme ISO 26000 - 7H
- Un cadre normatif largement reconnu : ISO 26000
- Les questions centrales

Examen certifiant « ISO 26000 Foundation »
- 1h, 50 questions QCM à livre fermé

Principes fondamentaux de la RSE et du DD -7H
- Généralités
- Mise en œuvre de la RSE selon l'ISO 26000

Evaluation de la performance d'une démarche RSE-7H
- Analyse de la matérialité
- Déploiement de la démarche RSE
- Evaluation & Notation de la RSE
- Reporting RSE

Mise en œuvre d'une démarche RSE - 7H
- Référentiels de Reporting
- Le reporting RSE: une activité en cours de réglementation
- La GRI: encadrement du reporting RS
- La pratique des rapports de DD
- Clôture de la formation

Examen certifiant « ISO 26000 Practitioner»
2h, 100 questions QCM à livre fermé



ISO 50001 FOUNDATION

Cette formation de 14 heures (réparties sur 2 jours) permet au participant de découvrir les fondamentaux du management de l'énergie, les concepts de base, et de comprendre un projet de mise en œuvre d'un SMEn . Au cours de cette formation l'apprenant acquerra la terminologie et les connaissances de base nécessaires sur la base des exigences de l'ISO 50001, au sein d'une organisation. Durant cette formation, participant acquerra la connaissance et les capacités de planifier, mettre en œuvre, évaluer et garantir l'intégrité d'un SMEN conformément aux exigences de la norme ISO 50001.

Public Cible

- Les spécialistes en gestion de l'énergie
- Toute personne intéressée par le domaine de la gestion de l'énergie
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au SMEn dans une organisation
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la gestion de l'énergie
- Membres d'une équipe projet en gestion de l'énergie
- Membre du personnel d'une organisation

Objectifs

- Comprendre les questions de gestion de l'énergie et sa mise en œuvre
- Acquérir les connaissances de base pour remplir les exigences de l'ISO 50001 dans le contexte d'une organisation
- Découvrir les bonnes pratiques de gestion de l'énergie et son lien avec la gestion des risques.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ENMS Foundation

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Les fondamentaux du management de l'énergie -7H
- Fondamentaux de la gestion de l'Energie
- Concepts de base et connaissances du contexte de l'organisation
- Leadership, Planification et support

La gestion des opérations du SMEN-7H
- Gestion des opérations du SMEN
- Évaluation de la performance
- Amélioration continue
- Processus de certification
- Révision et boite à outils

Examen certifiant « EnMS Foundation »
1h, 50 questions QCM à livre fermé



ISO 50001 LEAD IMPLEMENTER

Cette formation de 35 heures (réparties sur 5 jours) fournit aux participants l'occasion de découvrir le leadership d'un projet de mise en œuvre d'un SMEn et de préparer par la pratique à diriger des équipes opérationnelles dans le domaine du management de la Management de l'Energie. Pendant cette formation, participant acquerra la connaissance et les capacités de planifier, mettre en œuvre, évaluer et garantir l'intégrité d'un SMEn conformément aux exigences de la norme ISO 50001. Cette formation donne le droit à la certification Energy Management system Lead Implementer.

Public Cible

- Les spécialistes en gestion de l'énergie
- Toute personne intéressée par le domaine de la gestion de l'énergie
- Chefs de projets ou consultants souhaitant maîtriser les concepts associés au SMEn dans une organisation
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de la gestion de l'énergie
- Membres d'une équipe projet en gestion de l'énergie
- Membre du personnel d'une organisation voulant se préparer pour un poste en gestion de l'énergie

Objectifs

- Comprendre le fonctionnement d'un SMEn selon l'ISO 50001
- Développer les compétences nécessaires pour effectuer un projet de mise en œuvre d'un SMEn.
- Acquérir les compétences pour manager uneéquipe de projet pour lancer et maintenir un SMEn.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified EnMScLead Implmenter.

Prérequis

Une connaissance de base du management de l'énergie et de la norme ISO 50001 est nécessaire pour participer à ce cours.

Durée

35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits). L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Les fondamentaux du management de l'énergie - 7H
- Fondamentaux de la gestion de l'Energie
- Concepts de base et connaissances du contexte de l'organisation
- Leadership, Planification et support

La gestion des opérations du SMEn-7H
- Gestion des opérations du SMEN
- Évaluation de la performance
- Amélioration continue
- Processus de certification
- Révision et boite à outils

Examen certifiant « EnMS Foundation »
1h, 50 questions QCM à livre fermé

Le fonctionnement d'un SMEn tel qu'exigé par la norme ISO 50001-7h
- Etat des lieux
- Organisation du projet SMEn
- Comprendre l'organisation
- Référentiel documentaire du SMEn

La mise en œuvre d'un projet SMEn - 7h
- Gestion et traitement des risques
- Définir et mettre à jour les processus de management de l'énergie
- Formation, sensibilisation et communication
- Maitrise opérationnelle
- Gestion des achats

L'évaluation de la performance du SMEn et l'audit interne-7h
- Évaluation de la performance
- Audit interne et Revue de direction
- Amélioration continue
- Transfert aux opérations
- Processus de certification

Examen certifiant « EnMS Practitioner »
2h, 100 questions QCM à livre fermét



CERTIFIED ENERGY MANAGER

Cette formation certifiante de 35 heures offre aux participants l'occasion de monter en compétence sur l'optimisation de la performance énergétique d'une installation, d'un bâtiment ou d'un site industriel, à travers une certification reconnue de l'Association of Energy Engineers (AEE).
Au cours de cette formation, le participant acquerra les connaissances et compétences nécessaires pour analyser et améliorer la performance énergétique des installations, développer des compétences en gestion stratégique de l'énergie, identifier et mettre en œuvre des mesures d'efficacité énergétique, promouvoir des pratiques durables et responsables, et assurer la conformité aux normes et réglementations énergétiques en vigueur.

Public Cible

- Responsable de l'énergie souhaitant valider son expérience, ses connaissances
- Consultant ou fournisseur de service spécialisé en amélioration énergétique des bâtiments
- Propriétaire, gestionnaire d'un parc immobilier
- Ingénieur impliqué dans le développement de projets, stratégies, programmes en lien avec l'efficacité énergétique
- Énergéticiens, cadres
- Gestionnaires d'installations, de bâtiments
- Responsable développement durable

Objectifs

- Comprendre les questions de gestion de l'énergie et sa mise en œuvre
- Apprendre à analyser et améliorer la performance énergétique des installations
- Développer des compétences en gestion pour prendre des décisions éclairées et alignées avec les objectifs de l'organisation
- Identifier et mettre en œuvre des mesures d'efficacité énergétique pour réduire les coûts opérationnels
- Promouvoir des pratiques durables et responsables pour minimiser l'impact environnemental
- Assurer que les opérations respectent les normes et les réglementations énergétiques en vigueur
- Réussir l'examen de certification donnant droit à la désignation « Certified Energy Manager »

Prérequis

Cette formation nécessite :

- Des connaissances générales en énergie, en ingénierie ou en exploitation des installations techniques
- D'une expérience professionnelle dans les domaines de l'énergie, de la maintenance, des services techniques, de l'industrie, du bâtiment ou des utilités
- D'une compréhension des notions de base en électricité, thermique ou mécanique (recommandée)

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants. La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Introduction au management de l'énergie – 7H

- Approvisionnement en carburant
- Audits énergétiques
- Codes et standards

Comptabilité énergétique et systèmes électriques – 7H

- Comptabilité énergétique
- Systèmes d'alimentation électrique
- Moteurs et entraînements
- Systèmes d'éclairage
- Pratiques d'entretien et de mise en service

Systèmes du bâtiment et automatisation – 7H

- Systèmes HVAC
- Enveloppe du bâtiment
- Systèmes d'automatisation
- Stockage d'énergie

Systèmes industriels et contrats de performance – 7H

- Systèmes de chaudière
- Cogénération
- Systèmes industriels
- Contrats de performance
- Méthodes de mesure et de vérification

Validation des acquis et certification – 7H

- Validation des acquis
- Examen de certification

Examen certifiant « Certified Energy Manager »



CBAM (Mécanisme d'Ajustement Carbone aux Frontières)

Cette formation certifiante de 28 heures, officielle de l'EPD International, a été conçue pour fournir aux industriels, responsables RSE, responsables export, managers QHSE et décideurs les compétences techniques et réglementaires indispensables à une mise en conformité efficace et à une gestion proactive du risque carbone.

Public Cible

Cette formation s'adresse aux professionnels et organisations concernés par les exigences du CBAM et les obligations de reporting carbone liées aux exportations vers l'Union européenne.

Objectifs

- Identifier et calculer les émissions de GES selon le GHG Protocol (Scope 1 et Scope 2)
- Comprendre les fondamentaux de la gestion de l'empreinte carbone
- Maîtriser les principes et la méthodologie du CBAM
- Comprendre la relation entre le CBAM et le système EU ETS
- Évaluer les impacts du CBAM sur leur secteur d'activité
- Assurer un reporting conforme aux exigences européennes
- Intégrer la gestion carbone dans la stratégie export de l'entreprise

Prérequis

Aucune expertise approfondie en climat ou en marchés carbone n'est exigée.
Les concepts fondamentaux nécessaires à la compréhension du CBAM seront expliqués dès le premier jour.

Durée

Cette formation dure 28 heures, réparties sur 4 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.

Programme Détaille

Changement climatique et empreinte carbone – 7H

- Changement climatique et réchauffement global
- Changement climatique : menaces et opportunités pour les entreprises
- Concepts d'évaluation de l'empreinte carbone
- Sources des émissions de GES

Méthodologie et reporting GES – 7H

- Standards d'inventaire GES (GHG Protocol)
- Principes de reporting des inventaires GES
- Définition des périmètres organisationnels et opérationnels

Cadre réglementaire et fonctionnement du CBAM – 7H

- Système d'Échange de Quotas d'Émission de l'Union Européenne (EU ETS)
- Introduction au CBAM
- Fonctionnement du mécanisme (phase transitoire et phase définitive)
- Aspects réglementaires du CBAM
- Définitions clés
- Implications du CBAM pour les entreprises et les exportateurs

Mise en œuvre pratique & marchés carbone – 7H

- Méthodologie de calcul des émissions CBAM
- Études de cas sectorielles
- Exigences spécifiques par secteur
- Vérification CBAM
- Préparation à la conformité
- Relation entre CBAM et marchés carbone

Examen certifiant « CBAM »

Certification officielle EPD International



ESG MANAGER – ISO 26000, CSRD & CLIMAT

Face à l'accélération des exigences réglementaires européennes (CSRD, ESRS) et à la montée en puissance des enjeux climatiques et sociaux, cette formation certifiante de 35 heures vise à doter les participants des fondamentaux normatifs (ISO 26000), des compétences réglementaires (CSRD) et des outils méthodologiques clés (double matérialité, adaptation climatique) nécessaires pour piloter, déployer ou contribuer efficacement à une stratégie ESG. Cette formation prépare à la certification ESG Manager délivrée par Certi-Trust, attestant d'un socle de compétences reconnu et opérationnel.

Public Cible

- Responsables ou chargés RSE / ESG
- Managers, cadres dirigeants, responsables stratégie ou finance
- Consultants junior / confirmé en durabilité
- Auditeurs, QHSE, risk managers

Objectifs

- Comprendre et appliquer les principes de l'ISO 26000
- Maîtriser les exigences de la CSRD et des ESRS
- Réaliser une analyse de double matérialité conforme
- Identifier et intégrer les enjeux d'adaptation au changement climatique
- Structurer une démarche ESG cohérente et pilotable
- Contribuer à un reporting ESG fiable et réglementaire
- Se préparer et réussir l'examen de certification Certi-Trust

Prérequis

- Connaissances générales du fonctionnement d'une organisation
- Sensibilité aux enjeux de durabilité, RSE ou ESG
- Aucun prérequis technique ou réglementaire obligatoire

Durée

Cette formation dure 35 heures, réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Fondamentaux ESG & ISO 26000 – 7H
- Introduction à l'ESG et au développement durable
- Enjeux environnementaux, sociaux et de gouvernance
- Présentation de l'ISO 26000 : principes fondamentaux, parties prenantes, les 7 questions centrales
- Lien entre ISO 26000, ODD et ESG
- Atelier : identification des enjeux RSE d'une organisation

CSRD & cadre réglementaire européen – 7H
- Évolution du reporting extra-financier
- Présentation de la CSRD : champ d'application, calendrier, gouvernance et responsabilités
- Introduction aux ESRS : structure, thématiques clés
- Articulation CSRD – ISO 26000 – stratégie d'entreprise
- Étude de cas : analyse de conformité CSRD

Double matérialité (méthodologie & pratique) – 7H
- Définition et enjeux de la double matérialité
- Matérialité d'impact vs matérialité financière
- Méthodologie pas à pas : identification des enjeux, parties prenantes, évaluation et priorisation, documentation et validation
- Lien avec les ESRS
- Atelier pratique : construction d'une matrice de double matérialité

Adaptation climatique & stratégie ESG – 7H
- Changement climatique : notions clés
- Atténuation vs adaptation • Risques climatiques : physiques, de transition
- Intégration dans la stratégie et la gestion des risques
- Exigences ESRS E1 (approche simplifiée)
- Atelier : identification des risques climatiques et plan d'adaptation

Pilotage ESG, reporting & certification – 7H
- Construction d'un plan d'action ESG • Indicateurs et KPI ESG
- Organisation du reporting CSRD • Rôle et responsabilités de l'ESG Manager
- Révision générale et préparation à l'examen • Examen de certification Certi-Trust

Examen certifiant « ESG Manager – ISO 26000, CSRD & Climat »

Risque, conformité & anti-corruption

Gestion des risques

La gestion des risques permet aux organisations d'anticiper les menaces, de saisir les opportunités et de soutenir une prise de décision éclairée. Développer les compétences dans ce domaine contribue à renforcer la résilience, la performance et la pérennité des organisations.

Conformité

La conformité permet aux organisations de répondre aux exigences légales, réglementaires et normatives tout en renforçant leur gouvernance. Développer les compétences dans ce domaine favorise une culture de conformité, de responsabilité et d'amélioration continue.

Anti-corruption

La prévention de la corruption est un élément clé d'une gouvernance responsable. Développer les compétences dans ce domaine permet de promouvoir une culture d'intégrité, de transparence et d'éthique, tout en renforçant la confiance des parties prenantes.



ISO 31000 FOUNDATION

Cette formation de 14 heures (réparties sur 2 jours) offre aux participants l'occasion de monter en compétence sur les aspects principaux du Management des risques auxquels sont confrontés les organismes et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet d'un SMR dans le monde de l'organisme. Au cours de cette formation, l'étudiant acquerra les bases de connaissance et certaines aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de la gestion des risques.
Sur base de cas d'exemples et d'exercices pratiques, participant sera amené durant la formation à mieux cerner les aspects de planification, mise en œuvre, contrôle et amélioration d'un SMR en prenant en considération les exigences formelles de la norme et en interprétant adéquatement celles- ci dans une perspective de maîtrise des enjeux liés à la gestion des risques.

Public Cible

- Gestionnaires de risque
- Chefs de projets ou consultants souhaitant maîtriser la gestion des risques
- Responsables de la gestion d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de gestion des risques
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en gestion des risques

Objectifs

- Comprendre les principes du management du risque d'entreprise et sa mise en œuvre
- Acquérir les connaissances de base pour mettre en œuvre les lignes directrices de l'ISO 31000
- Découvrir les meilleures pratiques de management du risque d'entreprise dans le contexte de l'ISO 31000
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification Certified ISO 31000 Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

Cette formation dure 14 heures, réparties sur 2 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).

Programme Détaille

Gestion des risques selon la norme ISO 31000– 7H
- Fondamentaux du management des risques d'entreprises
- Leadership & Engagement
- Intégration, conception
- Mise en œuvre

Evaluation, processus, et appréciation du risque - 7H
- Evaluation et amélioration
- Processus de Gestion des Risques
- Communication et consultation
- Périmètre et contexte
- Appréciation du risque
- Traitement des risques
- Suivi et revue des risques
- Enregistrement et élaboration des Rapports d'évaluation de risque

Examen certifiant « ISO 31000 Foundation »
1h, 50 questions QCM à livre fermé



ISO 31000 RISK MANAGER CERTIFIÉ

Cette formation de 35 heures (réparties sur 5 jours) offre aux participants l'occasion de monter en compétence sur les aspects principaux du Management des risques auxquels sont confrontés les organismes et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet d'un SMR dans le monde de l'organisme. Au cours de cette formation, participant acquerra les connaissance et les aptitudes nécessaires pour comprendre les tenants et aboutissants des exigences de la gestion des risques sur la base de la normé ISO 31000.
Sur la base d'exemples réels et d'exercices concrets, participant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques selon la norme ISO 31000 tout en développant des capacités en gestion de programmes et de méthodes d'appréciation et de traitement ainsi qu'en ce qui concerne la gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Gestionnaires de risques
- Chefs de projets ou consultants souhaitant maîtriser la gestion des risques
- Responsables de la gestion d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de gestion des risques
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en gestion des risques

Objectifs

- Comprendre Les principes du management du risque d'entreprise et sa mise en œuvre
- Acquérir Les connaissances de base pour mettre en œuvre les lignes directrices de l'ISO 31000
- Découvrir les meilleures pratiques de management du risque d'entreprise dans le contexte de l'ISO 31000
- Mettre en œuvre un processus de gestion des risques en entreprise évaluer et améliorer le cadre de gestion des risques au sein de l'entre prise
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification Certified ISO 31000
- Risk Manager certifié.

Prérequis

Une connaissance de base en gestion des risques est nécessaire pour la participation à cette formation.

Durée

Cette formation dure 35 heures, réparties sur 5 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits)

Programme Détaille

Gestion des risques selon la norme ISO 31000– 7H
- Fondamentaux du management des risques d'entreprises
- Leadership & Engagement
- Intégration, conception
- Mise en œuvre

Evaluation, processus, et appréciation du risque - 7H
- Evaluation et amélioration
- Processus de Gestion des Risques
- Communication et consultation
- Périmètre et contexte
- Appréciation du risque
- Traitement des risques

Examen certifiant « ISO 31000 Foundation »
1h, 50 questions QCM à livre fermé

Le risque en entreprise entre surveillance et revue sur la base de la norme ISO 31000 - 7 H
- Comment accepter un risque en entreprise ?
- Suivi et revue des risques
- Enregistrement et élaboration des Rapports d'évaluation de risque
- Surveillance et contrôle du risque

Comment gérer et apprécier un risque conformément à la norme ISO31000 - 7 H
- Gestion du risque selon les exigences de la norme ISO 31000
- Évaluation du risque en entreprise
- Conclusion et clôture de la formation - 7 H
- Conclusions & Synthèse
- Clôture de la formation

Examen certifiant « ISO 31000 Risk Manager » 2
heures , 100 questions QCM à livre fermé



ISO 27005 RISK MANAGER

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la mise en œuvre d'un programme de gestion des risques en sécurité de l'information et de se préparer par la pratique à mener un projet de mise en œuvre d'un programme de gestion des risques conforme à la norme ISO/CEI 27005 : 2018 selon une méthode éprouvée.
Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à identifier, analyser, évaluer et traiter les risques dans le respect des exigences de l'ISO 27005 et de ses principaux processus.
Sur base d'exemples réels et d'exercices concrets, participant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques en sécurité de l'information tout en développant des capacités en gestion de programmes et de méthodes d'appréciation et de traitement ainsi qu'en ce qui concerne la gestion d'équipe, à travers la communication avec les différentes parties intéressées.

Public Cible

- Security Officer
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un système de management de la Sécurité de l'Information
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risque
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information

Objectifs

- Comprendre la relation entre la gestion des risques en sécurité de l'information et lesmesures de sécurité associées
- Assurer une gestion efficace des risques, à travers les concepts, approches, méthodes et techniques selon l'ISO 27005
- Développer des aptitudes sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISMS Risk
- Manager selon le niveau d'expérience.

Prérequis

Une connaissance de base de la Sécurité de l'Information et de la norme ISO 27001 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 21 heures, réparties sur 3 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 21 CPE (Continuous Professional Education credits).

Programme Détaille

Programme de gestion des risques selon la norme ISO/CEI 27005 : 2018 – 7H
- Gestion des risques en sécurité de l'information – concepts & principes fondamentaux
- Le cadre normatif de la gestion des risques
- La norme ISO/CEI 27005 : 2018
- Planification de la gestion des risques
- Le contexte de l'organisation et le périmètre de gestion des risques
- Mise en œuvre d'un programme de gestion des risques
- Approches de la gestion des risques
- Présentation de différentes méthodes de gestion des risques (toolbox)

Appréciation et traitement du risque en sécurité de l'information - 7H
- Identification des risques
- Analyse des risques
- Évaluation des risques
- Traitement du risque
- Relations entre ISO 27005 et ISO 27001
- Présentation et utilisation d'outils pratiques de gestion des risques (via étude de cas)

Activités de soutien et de surveillance des risques - 7H
- Documentation de la gestion des risques
- La communication sur le risque
- Les métriques d'évaluation de l'efficacité de la gestion des risques
- La réévaluation du risque
- L'amélioration continue de la gestion du risque
- Présentation et utilisation d'outils pratiques de gestion des risques (via étude de cas)

Examen certifiant « ISMS Risk Manager »
•2h,100 questions QCM à livre fermé



EBIOS RISK MANAGER

Cette formation de 21 heures offre aux participantsl'occasion de monter en compétence sur la mise en œuvre d'un programme de gestion des risques en sécurité de l'information et de se préparer par la pratique à mener un projet de mise en œuvre d'un programme de gestion des risques selon la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité).
Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à identifier, analyser, évaluer et traiter les risques dans le respect de la structure méthodologique propres à EBIOS et ses principaux processus. Sur base d'exemples réels et d'exercices concrets, participant sera progressivement amené durant la formation à assurer la bonne fin de la planification et gestion des risques en sécurité de l'information tout en développant des capacités en gestion de cette méthode d'appréciation et de traitement des risques en sécurité de l'information ainsi qu'en ce qui concerne la communication avec les différents intervenants

Public Cible

- Officiers de sécurité
- Gestionnaires de risque
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre de la méthodologie
- EBIOS en entreprise
- CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information ou de RSSI

Objectifs

- Comprendre le déroulement d'une approche en gestion des risques en sécurité de l'information basée sur EBIOS et les mesures méthodologiques associées
- Assurer une gestion technique efficace des risques à travers la méthode EBIOS
- Développer des aptitudes sur l'exécution de la méthode à travers des cas pratiques de gestion des risques liés à la sécurité de l'information
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified EBIOS Risk
- Manager selon le niveau d'expérience.

Prérequis

Une connaissance de base de la Sécurité de l'Information et de la norme ISO 27005 est nécessaire pour participer à ce cours.

Durée

Cette formation dure 21 heures, réparties sur 3 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 21 CPE (Continuous Professional Education credits).

Programme Détaille

Introduction à la méthode EBIOS - 7H
- Gestion des risques en sécurité de l'information – concepts & principes fondamentaux
- Cadre normatif de la gestion des risques
- La méthode EBIOS – Introduction, principes et concepts de base
- Les 5 phases de la méthode EBIOS
- Définition du cadre de la gestion des risques
- Identification des menaces, vulnérabilités, biens essentiels et biens de support
- Critères de sécurité et échelles de besoins, gravité et vraisemblance
- Appréciation des scénarios de menace
- Réalisation de l'appréciation des risques avec

EBIOS - 7H
- Analyse des risques
- Évaluation des risques
- Identification des objectifs de sécurité
- Choix des options de traitement du risque
- Relations entre ISO 27005 et EBIOS
- Formalisation des mesures de sécurité à mettre en œuvre

Activités de soutien et de surveillance des risques - 7H
- Exécution des traitements sur les risques
- Mise en oeuvre des mesures de sécurité
- Élaboration des plans d'action
- Analyse des risques résiduels
- Homologation de sécurité
- Cas pratique de gestion des risques (via étude de cas complète)

Examen certifiant « EBIOS Risk Manager »
2h – 100 questions QCM à livre fermé



ISO 37001 FOUNDATION

Cette formation offre aux participants l'occasion de monter en compétence sur les aspects principaux du management de l'anticorruption et de se familiariser avec les principes, méthodes et procédures appliquées au sujet d'un SMAC dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les connaissances de base et les aptitudes lui permettant de comprendre les tenants et aboutissants des exigences de la norme ISO 37001 pour la mise en œuvre d'une stratégie de management anti-corruption. Sur la base de cas d'exemples et d'exercices pratiques, participant sera amené durant la formation à mieux cerner les aspects de mise en œuvre d'une politique anti-corruption, en prenant en considération les exigences formelles de la norme ISO 37001.

Public Cible

- Les responsables qui veulent s'introduire à la mise en œuvre d'une stratégie anti-corruption
- Les dirigeants d'une entreprise souhaitant se familiariser avec les aspects relatifs au management de l'anticorruption
- Les membres du personnel d'une organisation voulant se préparer pour un poste en management de l'anticorruption

Objectifs

- Acquérir la terminologie et les connaissances nécessaires pour répondre aux exigences de l'ISO 37001 dans le contexte d'une entreprise
- Comprendre les enjeux du management de l'anti-corruption
- Découvrir les bonnes pratiques de mise en œuvre et de gestion d'un système anti-corruption
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 37001Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties.
À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
Laparticipation à cette formation donne droit à 14 CPE (Continuous Professional Education credits).
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™

Programme Détaille

Le SMAC tel qu'exigé par la norme ISO/CEI 37001 - 7 heures
- SMAC– concepts de base
- Principes fondamentaux du management anti-corruption
- Les principales clauses de l'ISO 37001
- Le contexte du SMAC au sein de l'entreprise
- Aspects de leadership et engagement managérial
- Planification d'un SMAC

Planification de la mise en œuvre d'un SMAC-7 heures
- Objectifs du management anti-corruption
- Champs d›application d›un SMAC
- Risques et opportunités

Examen certifiant « ISO 37001 Foundation »
1h, 50 questions QCM à livre fermé)



ISO 37001 LEAD AUDITOR

Cette formation ISO 37001 lead auditor offre aux participants l'occasion de monter en compétence sur la fonction d'assurance d'un système de management de l'anticorruption et de se préparer par la pratique à diriger d'autres auditeurs sur base de principes, de procédures et de techniques d'audits largement appliquées dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les bases de connaissance et les aptitudes l'autorisant à gérer une équipe d'auditeurs SMAC au sein de son entreprise sur la base des exigences de la norme ISO 37001 et de la norme ISO 19011. Sur base d'exemples réels et d'exercices concrets, participant aura l'occasion durant la formation à s'exercer pour mener l'audit d'un SMAC, à travers la meilleure gestion d'une équipe et la communication avec les différentes parties intéressées.

Public Cible

- Responsables d'un SMAC
- Directeurs recherchant un cadre complet de mise en œuvre du système de management anti-corruption
- Personnes voulant contribuer au maintien de l'intégrité organisationnelle en soutenant un comportement éthique.
- Membres de l'équipe de gestion d'un SMAC
- Chargé (e) voulant se préparer à un rôle de responsable d'un système de management anti-corruption.

Objectifs

- Maitriser les principes de la gestion d'un SMAC
- Développer les aptitudes nécessaires pour mener à bien un audit ISO 37001 dans le respect des exigences de l'ISO 19011.
- Acquérir la compétence de gestion d'une équipe d'auditeurs de SMAC
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 37001 Lead Auditor, selon le niveau d'expérience.

Prérequis

Une connaissance de base du management anti- corruption est nécessaire pour participer à ce cours.

Durée

Cette formation réparties sur 5 parties. À l'issue de la formation, un certificat de participation à la formation sera remis aux participants.
La participation à cette formation donne droit à 35 CPE (Continuous Professional Education credits).

Programme Détaille

Le SMAC tel qu'exigé par la norme ISO/CEI 37001 - 7 heures
- SMAC– concepts de base
- Principes fondamentaux du management anti-corruption
- Les principales clauses de l'ISO 37001
- Le contexte du SMAC au sein de l'entreprise
- Aspects de leadership et engagement managérial
- Planification d'un SMAC

Planification de la mise en œuvre d›un SMAC-7 heures
- Objectifs du management anti-corruption
- Champs d›application d›un SMAC
- Risques et opportunités

Examen certifiant « ISO 37001 Foundation »
1h, 50 questions QCM à livre fermé)



ISO 37301 FOUNDATION

Cette formation offre aux participants l'occasion de monter en compétence sur les aspects principaux du management de la conformité et de se familiariser avec les principes, méthodes et procédures appliquées au sein d'un Système de Management de la Conformité (SMC) dans le monde de l'entreprise. Au cours de cette formation, participant acquerra les connaissances de base et les aptitudes nécessaires pour comprendre les tenants et aboutissants des exigences de la norme ISO 37301, en vue de la mise en œuvre d'un système de management de la conformité efficace et durable. Sur la base de cas pratiques et d'exemples concrets, l'étudiant sera amené à mieux cerner les mécanismes de mise en place, d'évaluation et d'amélioration d'un système de management de la conformité, tout en intégrant les principes d'éthique, d'intégrité et de transparence prescrits par la norme ISO 37301. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore

Public Cible

- Les responsables qualité, conformité, audit interne ou juridique souhaitant s'initier à la mise en œuvre d'un système de management de la conformité.
- Les dirigeants et cadres d'entreprise voulant renforcer leur compréhension des enjeux liés à la conformité réglementaire et éthique.
- Les membres du personnel d'une organisation souhaitant se préparer à occuper un poste lié au management de la conformité.

Objectifs

- Acquérir la terminologie et les connaissances nécessaires pour répondre aux exigences de l'ISO 37301 dans le contexte d'une entreprise.
- Comprendre les enjeux du management de la conformité et son intégration dans la stratégie globale de l'organisation.
- Découvrir les bonnes pratiques pour concevoir, mettre en œuvre, surveiller et améliorer un système de management de la conformité (SMC).
- Réussir l'examen de CERTI-TRUST™.
- Solliciter la qualification de Certified ISO 37301 Foundation.

Prérequis

Aucun prérequis particulier n'est attendu pour la participation à cette formation.

Durée

14 heures, réparties sur 2 parties. À l'issue de la formation, un certificat de participation sera remis aux participants.
L'examen remplit l'ensemble des exigences du programme de certification CERTI-TRUST™.

Programme Détaille

Le SMC tel qu'exigé par la norme ISO 37301 – 7 heures
- Concepts de base du management de la conformité
- Principes fondamentaux d'un système de management de la conformité
- Les principales clauses de l'ISO 37301
- Le contexte du SMC au sein de l'entreprise
- Aspects de leadership et d'engagement de la direction
- Planification d'un SMC

Mise en œuvre et amélioration d'un SMC – 7 heures
- Détermination du champ d'application du SMC
- Évaluation des risques et opportunités en matière de conformité
- Mise en œuvre des processus de conformité et communication interne
- Surveillance, évaluation de la performance et amélioration continue

Examen certifiant « ISO 37301 Foundation »
(1h, 50 questions QCM à livre fermé)

Contact-Nous

+ 212 522 891 519
certification@certi-trust.com
www.certi-trust.com