CERTITRUST
LEARNING IN THE DIGITAL ERA

DIGITAL LEARNING
CATALOGUE

2021



Table de matière

Qui sommes nous ?

Certi-Trust est une marque de services de certification regroupant plusieurs compagnies agissant de manière indépendante qui effectuent certifient les professionnels et réalisent des audits de certification de systèmes de management, de produits et 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 ajouté et d'un panier diversifié de contenus certifiants, le tout encadré par des formateurs compétents et très spécialisés dans l'ensemble des domaines enseignés.

Notre vision

Devenir

un leader mondial des tests logiciels, de l'inspection et de la certification dans le domaine des technologies de l'information.

Notre mission

Participer

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

Nos valeurs

Compétence

Responsabilité – Transparence

Confidentialité – Réactivité.

CERTI-TRUST™ est la marque de certification qui accompagne la transformation numérique de nos clients dans le monde entier

La valeur de nos certifications

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.

Parce qu'il est essentiel pour un organisme de certification de personnes de prouver la conformité à une norme particulière, de garantir le respect des principes et des exigences, la cohérence et l'impartialité de la certification et de l'audit des services des systèmes de management, tous nos collaborateurs possèdent les qualifications professionnelles requises et sont constamment formés et encadrés pour fournir des services de haute qualité à nos clients. Certi-Trust et son personnel ne sont par ailleurs aucunement engagés dans une quelconque activité qui pourrait entrer en conflit avec leur indépendance de jugement, leur neutralité, leur impartialité ou leur intégrité par rapport aux services de certification qu'ils proposent.

Editorial

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 visio-conférence 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).*

C’est donc dans ce contexte changeant et très rapidement évolutif que nous avons développé une plateforme de Digital Learning innovante pour réaliser nos formations préparatoires aux certifications proposées par Certi-Trust. Tout d'abord l’ensemble de nos cours est conçu pour engager véritablement nos apprenants et augmenter le taux de rétention à travers notamment la mise en pratique de recherches en neurosciences et l'utilisation de différents outils de production de contenu complémentaires et fortement innovants, choisis avec soin par nos équipes pédagogiques, dans ce que nous appelons la « Pédagogie Digitale Augmentée ». Ensuite, nos formateurs partenaires ou organismes de formation affiliés sont eux-mêmes formés et accompagnés par nos équipes techniques et pédagogiques pour homogénéiser et fluidifier l’expérience sous-toutes ses formes. Enfin, la plateforme peut aussi bien s’utiliser dans des parcours 100% en ligne qu’à l’occasion de classes hybrides (une partie en présentiel, une partie en ligne) ou totalement présentielles, dans des dispositifs de classe inversée, notamment.

Mot du CEO

"Les presque deux 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.

Las, 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 professeur et formateur dans le domaine des technologies de l'information depuis 25 ans.

Mot du CEO

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 (c'est devenu assez flou depuis 18 mois) d'une façon relativement inédite.

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.

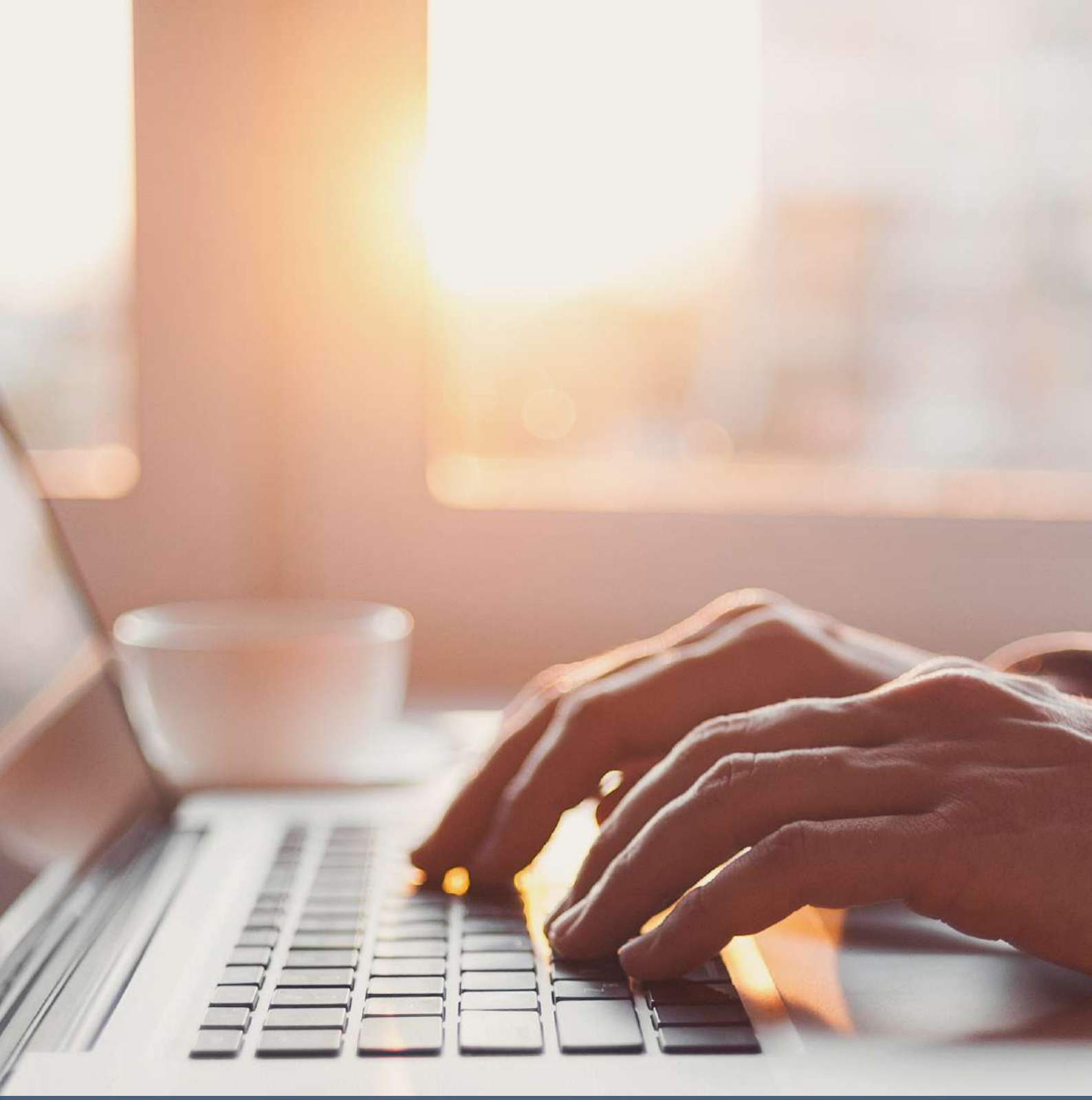
Le leitmotiv de « CTDL » est ainsi devenu, en écho à notre slogan d'entreprise, « Confiance dans l'apprentissage numérique ».

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.

Bien sincèrement,

Pierre Dewez
CEO Certi-Trust Groupe



Certi-Trust
Digital learning platform

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

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 minimum de 4 mois.**

- **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 (tchat individualisé, forum partagé, session live, questions/réponses intégrées au capsule) enrichissent et personnalisent l'expérience utilisateur.**

Recherchez vous le meilleur moyen de développer vos connaissances et vos compétences ?

CTDL La plateforme de digital learning la plus interactive au Monde.

- Des formations certifiantes en Français et en Anglais
- Des formateurs agréés

Découvrez nos formations 3.0 !

- Des sessions live
- Des vidéos enrichies
- Des tests en ligne
- Un forum

Et décrochez les certificats les plus prestigieux

Nous vous préparons à relever vos défis professionnels

Devenez la meilleure version de vos mêmes !

Contactez-nous via : education@certi-trust.online

Outils mis à disposition :

Certi-Trust Digital Learning met à disposition un ensemble d'outils construits et choisis méticuleusement pour engager l'apprenant:

01 Un support de formation, sous forme d'un diaporama numérique interactif, enrichi avec des quizzes et des exercices de compréhension intégrés au fil de la lecture.

02 Un espace « live session » au sein duquel les étudiants et le formateur pourront se retrouver pour échanger en direct à travers :

a. Un partage d'écran du formateur
b. Un module vidéo permettant de lancer des séquences filmées pour illustrer un cas d'étude
c. Un tableau blanc sur lequel le formateur pourra écrire en temps réel durant la « live session »
d. Un chat en temps réel (archivable par chacun)

03 Un agenda de formation pour permettre aux étudiants de gérer leurs rendez-vous « live sessions » et ateliers collaboratifs. L'agenda permet de :

1. Connaître quand les « live sessions » ont lieu et de s'y inscrire
2. Prendre rendez-vous avec le formateur pour des séances de questions réponses collectives ou individuelles
3. Connaître les échéances de remise des travaux individuels et de groupes proposés par le formateur

04 Un forum dans lequel les étudiants pourront poser des questions et interagir de manière asynchrone avec le formateur et leurs pairs sur tous les sujets liés à la formation.

05 Des séquences vidéos explicatives de 10 mins enregistrées par nos différents formateurs spécialisés, chacun présentant synthétiquement la matière et les points importants tout résumant, à la fin de chaque chapitre, les différents points de matière à retenir.

06 Tous les exercices individuels et collectifs préparatoires à l'examen de certification associé, sous forme de :

1. QCM préparatoires aux examens de certification (tests à blanc)
2. Questionnaires ouverts à corriger en groupe avec le formateur lors des « live sessions »
3. Questionnaires ludico-interactifs à réaliser en groupe lors des « live sessions » avec le formateur

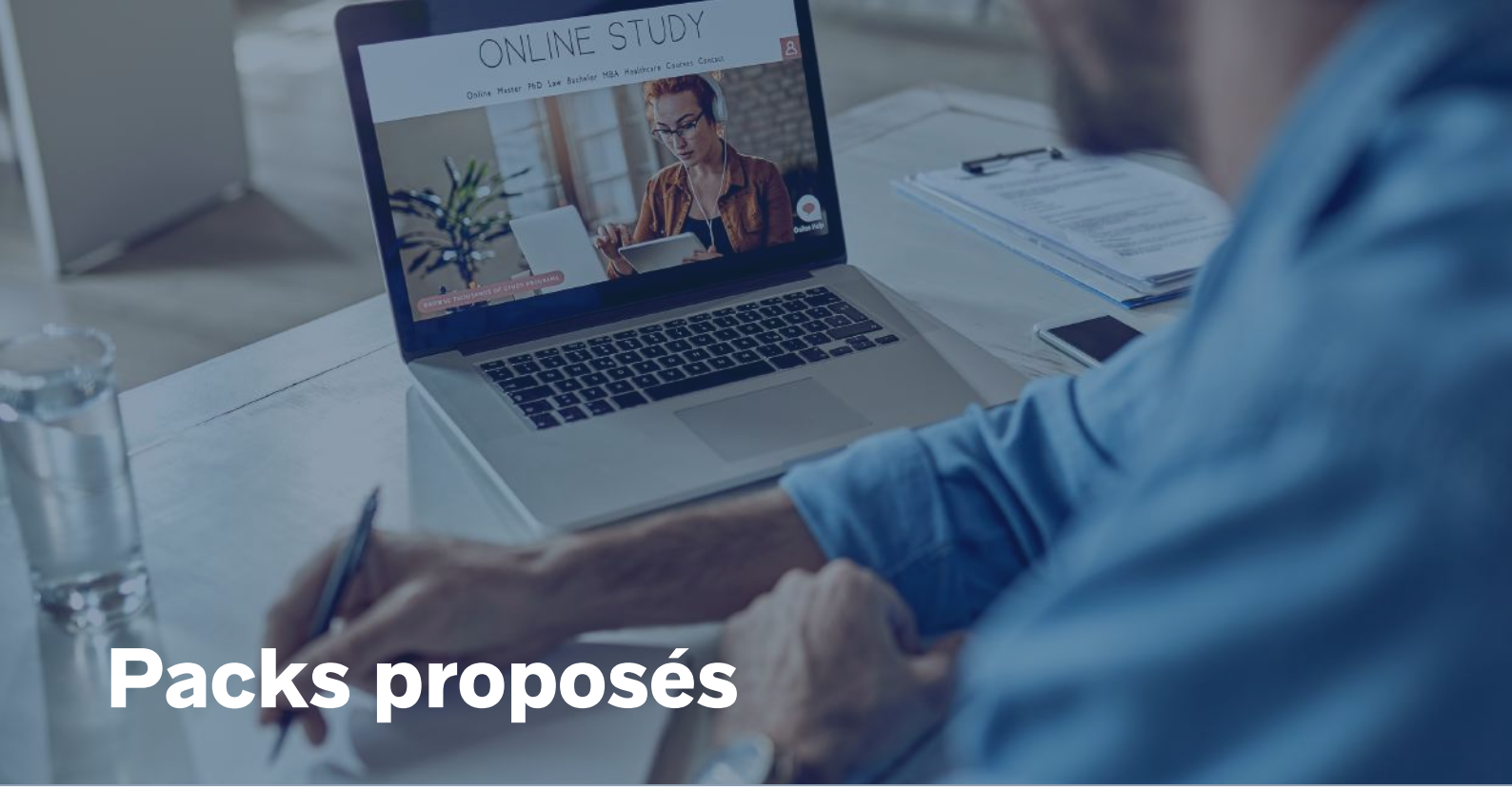
07 Espaces « ateliers » pour les travaux de groupe (études de cas, notamment) distribués par le formateur aux stagiaires.

08 Flash cards thématiques qui synthétisent, en fin de chapitre, la matière abordée, au fur et à mesure du parcours d'apprentissage, en complément de la synthèse présentée par le formateur.

09 Un examen à blanc par cours préparatoire à la certification, sous forme de QCM et d'une longueur variable selon le cours concerné (de 25 à 125 questions).

10 Toutes les notes et références additionnelles utiles fournies par le tuteur/formateur, que ce soit en accompagnement du support de formation ou sous forme de documents stockés dans l'espace de formation du stagiaire.

11 Des guides pour pouvoir naviguer dans l'espace de formation, gérer son agenda de formation et se connecter aux « live sessions » planifiées et animées par le(s) formateur(s).



Packs proposés

Pack Basic	Pack Pro	Pack Premium
E-LEARNING		
• support de cours • exercices qcm • Exercices ouverts • flash-cards • notes et références	• support de cours • exercices qcm • Exercices ouverts • flash-cards • notes et références • examen à blanc • agenda • forum • capsules vidéos • tchat temps réel • tutorat interactif	• support de cours • exercices qcm • Exercices ouverts • flash-cards • notes et références • examen à blanc • agenda • forum • capsules vidéos • tchat temps réel • tutorat interactif • atelier collaboratif • tableau blanc • sessions « live » • examen certifiant
4 Mois	**8 Mois**	**12 Mois**

Nos examens de certification

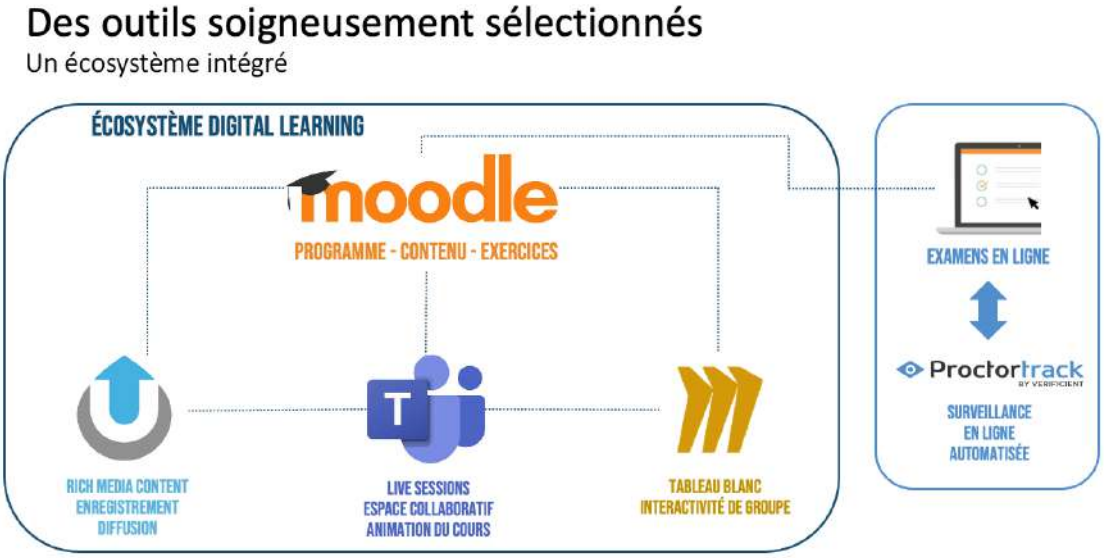
Des examens de certification pour valider vos compétences !

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.

Des examens sous haute (mais juste) surveillance

Le système de surveillance d'examens que Certi-Trust utilise (ProctorTrack®) est totalement intégré à la plateforme d'évaluation et le candidat est accompagné durant toute la phase préparatoire à l'examen par un ensemble d'instructions claires et documentées lui permettant d'accéder rapidement et efficacement à son examen après s'être identifié et authentifié sur le portail de validation.

La surveillance des examens se déroule de deux manières différentes selon le schéma de certification proposé et le grade à obtenir : de façon automatisée ou sous la supervision d'un membre de Certi-Trust.

Tous les examens de base sont soumis à une surveillance automatisée, guidée par une intelligence artificielle, qui permet au candidats inscrits de présenter un examen quand ils le souhaitent, même en dehors des heures de bureau (à condition bien sûr de s'inscrire préalablement auprès de nos services).

Le système encadre le candidat durant toute la séance d'examen et pré-valide la passation de l'examen si les conditions de ce passage ont été respectées. Une modération humaine intervient toujours suite au passage de ce type d'examens pour valider que le système est resté efficace et 'fair-play' avec chaque candidat. En cas de doute, nous proposons systématiquement aux candidats de repasser gratuitement l'examen auquel ils auraient éventuellement échoué suite à une décision inadéquate du système.

Les examens complexes (hors QCM, par exemple) sont soumis à une surveillance humaine permanente doublée d'une surveillance par IA pour optimiser le processus d'inscription des candidats et épauler le surveillant dans ses activités. Lorsque le candidat passe un tel examen, il est supervisé par un membre de l'équipe de gestion des examens de Certi-Trust qui valide sa participation, surveille le passage de l'examen et agit en support du candidat si un problème survient éventuellement lors du passage de l'examen. Il est cependant à noter que les surveillants ne peuvent jamais aider les candidats à répondre aux questions et qu'ils ne sont pas habilité à se prononcer sur les contenus des examens, à aucun moment.

L'ensemble des données collectées durant la phase d'inscription et l'examen lui-même ne sont conservées de manière individuelle que pendant le temps strictement nécessaire à la passation de l'épreuve et à la validation des résultats du candidat et/ou la gestion d'éventuelles contestations comme stipulé dans nos manuels des candidats pour chaque schéma évalué. Toutes les données personnelles sont ensuite détruites et Certi-Trust ne conserve que les données signalétiques des personnes, les résultats chiffrés des examens et le dossier professionnel pendant toute la durée de validité de la certification de chaque candidat. Ces données peuvent évidemment donner lieu à demande d'information, de modification ou même de suppression (entraînant alors de facto le retrait de la certification, le cas échéant) à la demande du candidat. Elles ne sont jamais transférées à des tiers ni utilisées à d'autres fins que celles pour lesquelles elles ont été initialement collectées.

Vous avez aimé notre expérience d'examen ? Aidez-nous maintenant à encore mieux interroger d'autres candidats !

Lorsqu'un candidat a réussi un examen et obtenu son grade de certification professionnelle chez Certi-Trust, il peut, s'il le souhaite, participer avec toute la communauté des professionnels certifiés, à la rédaction de nouvelles questions d'examens. Cette participation lui offre, outre la possibilité de pouvoir passer en avant-première tous nos nouveaux examens pilotes, de collecter des Crédits d'Éducation Professionnelle (CPE) pour cette participation. N'hésitez pas à interroger nos équipes à ce sujet. On compte sur vous !

Si vous souhaitez nous contacter pour passer un examen ou pour toute question relative à notre plateforme d'évaluation, écrivez-nous à examination@certi-trust.com ou surfez sur notre site web www.certi-trust.com, dans le menu « Certification de personnes – Examens ».

Rendez-vous très bientôt sur notre plateforme pour évaluer vos compétence !
L'équipe d'Examens.

Information Security

À PROPOS

De nos jours, détecter et faire face aux menaces ciblant les informations devient crucial pour tout type d'entreprise.

C'est dans cette perspective que nous offrons 3 formations liées directement à la sécurité des systèmes d'information, afin d'aider les professionnels à savoir comment bien protéger leurs données.

FORMATIONS DISPONIBLES

- ISMS Foundation
- ISMS Lead Implementer
- ISMS Lead Auditor

ISMS Foundation

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la gestion de la sécurité de l'information et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du SMSI 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 27001 pour la mise en œuvre et les opérations d'un SMSI. 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 SMSI 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 de l'Information 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 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'information

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-TRUST™
- 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'ensemble des exigences du programme de certification CERTI-TRUST™

Agenda général

- Le SMSI tel qu'exigé par la norme ISO/CEI 27001:2013 - 7h
- Fonctionnement du SMSI + Outils de gestion du cycle de vie d'un SMSI - 7h
- Examen ISMS Foundation (1h – 50 questions QCM)

L'examen « ISMS Foundation », composé d'un total de 50 questions à choix multiple et d'une durée totale de 1 heure, à livre fermé, atteste du fait que le candidat dispose des connaissances et aptitudes pour comprendre les enjeux liés à un SMSI ainsi que les termes et conditions de son mise en œuvre, de son exécution, de sa surveillance et de son amélioration continue en fonction des exigences de la norme ISO/CEI 27001:2013.

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISMS Lead Implementer (21 heures)
- ISMS Lead Auditor (21 heures)

Ils peuvent être suivis consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

Le SMSI tel qu'exigé par la norme ISO/CEI 27001:2013 - 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)

ISMS 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 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 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 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 ISO 27001
- 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

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).

Agenda général

- Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2013 - 7h
- Fonctionnement du SMSI + Outils de gestion du cycle de vie d'un SMSI - 7h
- Examen ISMS Foundation (1h – 50 questions QCM)
- Planifier la mise en œuvre d'un SMSI - 7h
- Mener les opérations & mesurer la performance du SMSI - 7h
- Assurer la pérennité du SMSI au cours du cycle de vie + Exercices - 7h préparatoires supplémentaires (QCM & questions ouvertes)
- Examen ISMS Practitioner (2h – 100 questions QCM)

Cette formation se compose de 2 modules distincts :

- ISMS Foundation (14 heures)
- ISMS Practitioner (21 heures)

Ils peuvent être suivis séparément l'un de l'autre ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 500 pages de contenu, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2013 – 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)

ISMS 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, l'étudiant 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 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 ISO 27001
- 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).

Agenda général

- Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2013 – 7 heures
- Fonctionnement du SMSI + Outils de gestion du cycle de vie d'un SMSI – 7 heures
- Examen ISMS Foundation (1 heure – 50 questions QCM)
- Planifier et mettre en œuvre un audit de SMSI – 7 heures
- Mener un audit de SMSI – 7 heures
- Clôturer et assurer le suivi d'un audit de SMSI + Exercices préparatoires supplémentaires (QCM & questions ouvertes) – 7 heures
- Examen ISMS Auditor (2 heures – 100 questions QCM)

Cette formation se compose de 2 modules distincts :

- ISMS Foundation (14 heures)
- ISMS Auditor (21 heures)

Ils peuvent être suivis séparément l'un de l'autre ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

Le SMSI tel qu'exigé par la norme ISO/CEI 27001 : 2013 – 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 de l'audit d'un 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.

Risk Management

À PROPOS

Dans un monde où la gestion des risques devient de plus en plus importante. Nous agissons en tant que tiers de confiance des entreprises, en leurs aidant à mieux comprendre les meilleures pratiques de la gestion des risques liée aux systèmes d'information. en leurs offrant 2 formations spécialisées dans ce domaine.

FORMATION DISPONIBLE

- ISMS Risk Manager
- EBIOS Risk Manager

ISMS 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, l'étudiant 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, 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 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 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).

Agenda général

- Gestion des risques selon la norme ISO/CEI 27005:2018
- Identification, analyse et évaluation des risques
- Traitement des risques et réévaluation des risques + Outils de gestion des risques en sécurité de l'information
- Examen ISMS Risk Manager (2h – 100 questions QCM)

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISMS Foundation (14 heures)
- ISMS Implementer (21 heures)
- ISMS Auditor (21 heures)

Ils peuvent aussi être combinés avec d'autres modules de notre catalogue. N'hésitez pas à nous interroger à ce sujet. Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTITRUST™.

Programme détaillé

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, l'étudiant 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 risques
- 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).

Agenda général

- Introduction à la gestion des risques selon EBIOS
- Réalisation de l'appréciation des risques avec EBIOS
- Traitement des risques et réévaluation des risques + Exercices pratiques sur une étude de cas
- Examen EBIOS Risk Manager (2h – 100 questions QCM)

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISO 27001 Foundation (14 heures)
- ISO 27005 Risk Manager (21 heures)
- ISO 27001 Lead Auditor (21 heures)
- ISO 27001 Lead Implementer (21 heures)

qui peuvent aussi être combinés avec d'autres modules de notre catalogue. N'hésitez pas à nous interroger à ce sujet.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel de soutien sont fournis sous licence Creative Commons (CC) par CERTI-TRUST™

Programme détaillé

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

Privacy

À PROPOS

Mieux comprendre le règlement général de protection des données à caractère personnel et découvrir ses bonnes pratiques représentent les 2 facteurs clés pour lesquels nous vous proposons 3 formations dans le domaine de la protection des données.

FORMATIONS DISPONIBLES

- RGPD Foundation
- Data protection officer
- ISO 27701 Foundation

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, l'étudiant 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
- Avocats, juristes
- Conseillers experts en protection des données personnelles

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 Data Protection Officer selon le niveau d'expérience.

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™

Agenda général

- La Protection des Données et le RGPD - 7H
- Les composants du RPGD et les relations qu'ils entretiennent - 7H

Examen certifiant « GDPR Foundation »

- 1h, 50 questions QCM à livre fermé

L'examen « GDPR Foundation», composé d'un total de 50 questions à choix multiple et d'une durée totale de 1 heure, à livre fermé.

Cette formation peut se combiner avec un autre module distinct comme :

- Data protection Officer (21 heures)

Ils peuvent être suivis consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

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 données
- 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

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 - Certified Data Protection Officer a été développé pour, sur base d'exemples réels et d'exercices concrets, donner à l'étudiant les connaissances et aptitude lui permettant de mener à bien la mise en œuvre d'un programme de conformité de la protection des données à caractère 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 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
- 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).

Agenda général

- Le RGPD – concepts, principes et cadre légal (y compris local, pays par pays) - 7h
- Conformité, Imputabilité, transferts internationaux et rôle du Délégué à la
- Protection des données + Exemples de documents utiles pour répondre au RGPD - 7h

Examen GDPR Foundation (1h – 50 questions QCM)

- Réglementation par la pratique, obligations des acteurs, analyse des risques et aspects de Sécurité de l'Information - 7h
- Appréciation des impacts sur la protection des données (étude de cas et livrables associés) - 7h
- Outils et techniques à mettre en œuvre pour assurer la protection effective des données + Exercices préparatoires (QCM & questions ouvertes) - 7h

Examen Data Protection Officer (2h – 100 questions QCM)

Cette formation se compose de deux modules distincts :

- GDPR Foundation (14 heures)
- Data Protection Officer (21 heures)

Ils peuvent être également combinés avec d'autres modules de notre catalogue.
Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

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

ISO 27701 Foundation

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 sur la base de la norme internationale ISO 27701, et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet de la protection des données à caractère personnel dans le monde de l'entreprise.
Au cours de cette formation, l'étudiant acquerra la connaissance et les compétences pour comprendre les tenants et aboutissants des exigences de l'ISO 27701.

Public cible

- Chefs de projet ou consultants souhaitant accompagner une organisation dans la mise en œuvre et l'adoption des nouvelles exigences de la norme ISO 27701.
- Les responsables qui souhaitent comprendre la norme ISO 27701
- 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
- Avocats, juristes
- Conseillers experts en protection des données personnelles

Objectifs

- Comprendre les enjeux de la protection des données selon la norme ISO 27701 et sa mise en œuvre.
- Acquérir la terminologie et les connaissances de base nécessaires pour remplir les exigences de l'ISO 27701.
- Découvrir les bonnes pratiques de gestion des données à caractère personnel.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified Data Protection Officer selon le niveau d'expérience.

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™

Agenda général

- La terminologie, les concepts clés et les principes fondamentaux de l'ISO 27701 - 7H
- Gouvernance et traitement des données à caractère personnel au sein d'une organisation sur la base des exigences de l'ISO 27701 - 7H

Examen certifiant « ISO 27701 Foundation »

- 1h, 50 questions QCM à livre fermé

L'examen « ISO 27701 Foundation», composé d'un total de 50 questions à choix multiple et d'une durée totale de 1 heure, à livre fermé.

Cette formation peut se combiner avec un autre module distinct comme :

- ISO 27701 Practitioner (21 heures)

Ils peuvent être suivis consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

La terminologie, les concepts clés et les principes fondamentaux de l'ISO 27701 - 7H

-
-

Gouvernance et traitement des données à caractère personnel au sein d'une organisation sur la base des exigences de l'ISO 27701 - 7H

-
-

Examen certifiant « ISO 27701 Foundation »

- 1h, 50 questions QCM à livre fermé

La continuité d'activité

À PROPOS

Dans un contexte de crise sanitaire mondiale, se former à la continuité d'activité pour assurer la survie de son entreprise est une nécessité !

C'est pourquoi, nous vous offrons une formation d'initiation et 2 formations de spécialisation dans ce domaine.

FORMATIONS DISPONIBLES

- BCMS Foundation
- BCMS Lead Implementer
- BCMS Lead Auditor

BCMS 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, l'étudiant 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™

Agenda général

- Le SMCA tel qu'exigé par la norme ISO 22301 : 2012 – 7h
- Fonctionnement du SMCA + Outils de gestion du cycle de vie d'un SMSI - 7

Examen BCMS Foundation - 1h – 50 questions QCM

Cette formation peut se combiner avec d'autres modules distincts comme BCMS Lead Implementer (21 heures) et BCMS Lead Auditor (21 heures) qui peuvent être suivis consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

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 SMSI – 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

BCMS
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 les aptitudes 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, l'étudiant 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, 27031 et 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).

Agenda général

- Le SMCA tel qu'exigé par la norme ISO 22301 : 2019 - 7h
- Fonctionnement du SMCA + Outils de gestion du cycle de vie d'un SMCA. - 7h
- Examen BCMS Foundation (1h – 50 questions QCM)
- Planifier la mise en œuvre d'un SMCA 4e jour Mener les opérations & mesurer la performance du SMCA. - 7h
- Assurer la pérennité du SMCA au cours du cycle de vie + Exercices préparatoires supplémentaires (QCM & questions ouvertes) - 7h
- Examen BCMS Practitioner (2h – 100 questions QCM)

Cette formation se compose de deux modules distincts :

- BCMS Foundation (14 heures)
- BCMS Practitioner (21 heures)

Ils peuvent être suivis séparément l'un de l'autre ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

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

BCMS 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 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, l'étudiant 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 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).

Agenda général

- Le SMCA tel qu'exigé par la norme ISO 22301 : 2019 – 7H
- Fonctionnement du SMCA + Outils de gestion du cycle de vie d'un SMCA - 7H
- Examen BCMS Foundation (1h – 50 questions QCM)
- Planifier et mettre en œuvre un audit de SMCA – 7H
- Mener un audit de SMCA – 7H
- Clôturer et assurer le suivi d'un audit de SMCA + Exercices préparatoires supplémentaires (QCM & questions ouvertes) – 7H
- Examen BCMS Auditor (2h – 100 questions QCM)

Cette formation se compose de deux modules distincts, BCMS Foundation (14 heures) BCMS Auditor (21 heures) qui peuvent être suivis séparément l'un de l'autre ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

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

Cybersecurity

À PROPOS

la protection des données numériques d'une organisation est un facteur clé de sécurité de son système d'information contre les cybermenaces.
Pour réaliser ce but de protection des données, nous vous proposons 3 formations d'actualité dans le domaine de la cybersécurité.

FORMATIONS DISPONIBLES

- Cybersecurity Practitioner
- Cloudsecurity Practitioner
- Rôle du RSSI

Cybersecurity Practitioner

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, l'étudiant acquerra 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, l'étudiant 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 Practitioner 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).

Agenda général

- Le programme de Cybersécurité tel que défini par le NIST Cybersecurity Framework et l'ISO/CEI 27032:2012 - 7H
- Cyberattaques et exposition des organisations - Fonctionnement d'un programme de Cybersécurité selon le NIST et d'autres référentiels clés + Outils de gestion du cycle de vie d'un programme de Cybersécurité (toolbox) - 7H
- Examen Cybersecurity Foundation (1h – 50 questions QCM)
- Planifier la mise en œuvre d'un programme de Cybersécurité (LAB) - 7H
- Mener les opérations & mesurer la performance des composants du programme de Cybersécurité (LAB)- 7H
- Assurer la pérennité du programme de Cybersécurité au cours de son cycle de vie + Exercices préparatoires supplémentaires (QCM & questions ouvertes) - 7H
- Examen Cybersecurity Practitioner (2h – 100 questions QCM)

Cette formation se compose de deux modules distincts :

- Cybersecurity Foundation (14 heures)
- Cybersecurity Practitioner (21 heures)

qui peuvent être suivi séparément l'un de l'autre ou combinés avec d'autres modules de notre catalogue, comme SCADA SECURITY PRACTITIONER, PENTEST FOUNDATION-PRACTITIONER, CLOUD SECURITY PRACTITIONER, ISO 27001 LEAD AUDITOR-LEAD IMPLEMENTER.

Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons (CC) par CERTI-TRUST™

Programme détaillé

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)

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 Practitioner

Cette formation de 21 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 sécurité du Cloud basé sur ISO 27017 et ISO 27018 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 programme de sécurité du Cloud computing pour son organisation dans le respect des meilleures pratiques associées. Sur base de labs pratiques, d'exemples réels et d'exercices concrets basés sur des environnements à simulation technique avancée, l'étudiant sera amené durant la formation à mener à bien un projet d'implémentation d'un programme de sécurité du Cloud en développant des capacités en architecture des environnements, en gestion de programme, de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées et spécialement les fournisseurs de services IaaS, PaaS et SaaS dans le Cloud.

Public cible

- 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

- Maîtriser les concepts, approches, normes, méthodes et techniques pour participer à la mise en œuvre et la gestion d'un programme de sécurité du Cloud conforme aux meilleures pratiques au sein d'une organisation selon ISO 27017 et 27018
- Comprendre le but, le contenu et la corrélation entre la Sécurité de l'Information et le cadre de sécurité du Cloud ainsi qu'avec d'autres normes et standards de l'industrie
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques de gestion de la sécurité du Cloud
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified Cloud Security Practitioner 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 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).

Agenda général

- Définir et mettre en œuvre un référentiel pour la gestion d'un programme de sécurité Cloud en prenant en considération les risques sur la chaîne d'approvisionnement et les relations avec les fournisseurs de solutions infonuagiques. - 7H
- Aspects de sécurité liés à l'acquisition, le développement et la maintenance de solutions Cloud, la sécurité des communications - 7H
- Gestion des incidents, aspects de continuité et architectures 'Cloud' de référence + Cas pratique d'étude & Examen à blanc - 7H
- Examen Cloud Security Practitioner (2h – 100 questions QCM)

Cette formation peut se combiner avec d'autres modules distincts comme :

- Cybersecurity Foundation (14 heures)
- ISO 27001 Foundation (14 heures)
- ISO 22301 Foundation (14 heures)

qui peuvent être suivis consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue comme CYBERSECURITY PRACTITIONER, ISO 27001 LEAD IMPLEMENTER-AUDITOR, ISO 22301 LEAD IMPLEMENTER-AUDITOR.

Le support de cours officiel (composé de plus de 300 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons (CC) par CERTI-TRUST™ –> voir les conditions d'utilisation complètes sur notre site www.certi-trust.com.

Programme détaillé

- Définition et mise en œuvre d'un programme de sécurité du Cloud - 7H
- Objectifs et structure du cours
- Concepts et définitions – les types d'environnements 'Cloud'
- Référentiels, cadre normative et meilleures pratiques basés sur ISO 27017 et 27018
- Mettre en œuvre un référentiel de gestion du Cloud dans une organisation
- Compréhension de l'organisme et de son contexte
- Pourquoi gérer la sécurité du Cloud ?
- Concepts, modèles et risques
- Mesures de sécurité dans le Cloud & contrôle des fournisseur
- Assurance sur la fourniture sécurisée de services Cloud
- Processus de gestion de la chaîne d'approvisionnement
- Politiques de sécurité
- Organisation de la Sécurité de l'Information dans un environnement 'élastique'
- Protection des informations personnellement identifiables (PII)
- Sécurité des ressources humaines et des actifs
- Contrôle d'accès aux ressources
- Outils de support d'un programme de sécurité du Cloud (documentation, ressources, etc.)

Gestion des infrastructures et des communications dans le Cloud - 7H

- Sécurité des communications et aspects de cryptographie
- Sécurité des opérations en modes IAAS, PAAS, SAAS
- Acquisition, développement et maintenance de solutions basées sur le Cloud
- Présentation de la documentation nécessaire aux opérations du programme (toolbox)

Gestion des infrastructures et des communications dans le Cloud - 7H

- Gestion des incidents, leurs conséquences et la réponse à y apporter
- Gestion de la continuité des opérations grâce au Cloud
- Quelques architectures sécurisées Cloud de référence
- Exercices pratiques sur un cas d'étude
- Préparation à la certification
- Examen à blanc

Examen certifiant « Cloud Security Practitioner » (2h – 100 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 équipes 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, l'étudiant 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, l'étudiant 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.

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).

Agenda général

- Gouvernance globale de la SSI - 7H
- Gestion des risques - 7H
- Gestion de la sécurité opérationnelle - 7H
- Aspects légaux de la SSI - 7H
- Cybersécurité opérationnelle (exemple) - 7H
- Examen RSSI Certifié (3h – 100 questions QCM – 10 questions ouvertes)

Cette formation se compose de trois modules complémentaires:

- Gouvernance de la Cybersécurité (21 heures)
- Aspects légaux du rôle de RSSI (7 heures)
- Cybersécurité Pratique (7 heures)

qui peuvent être suivis distinctement l'un de l'autre ou combinés avec d'autres modules de notre catalogue, comme SCADA SECURITY PRACTITIONER, PENTEST FOUNDATION-PRACTITIONER, CLOUD SECURITY PRACTITIONER, ISO 27001 LEAD AUDITOR-LEAD IMPLEMENTER.

Le support de cours officiel (composé de plus de 400 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (étude de cas, exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons (CC) par CERTI-TRUST™ –

Programme détaillé

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 (ISO 27001 et normes assimilées)
- 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
- Le support d'un programme SSI (documentation, ressources, etc.)

Gouvernance SSI – partie 2 : La gestion des risques (7 H)

- Vecteurs d'attaque communs, agents de menaces, motifs et types d'attaques
- Threat Intelligence et appréciation des risques SSI
- 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 Sécurité Opérationnelle)

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 10 questions ouvertes)

Application Security

À PROPOS

Le processus de sécurité des applications prouve davantage jour après jour une grande performance au niveau de la protection des données au sein des entreprises.
Dans ce ses, nous proposons dans ce domaine, une formation de base et 2 formations de spécialité.

FORMATIONS DISPONIBLES

- ISO 27034 Foundation
- ISO 27034 Practitioner
- ISO 27034 Auditor

ISO 27034 Foundation

Cette formation de 14 heures offre aux participants l'occasion de monter en compétence sur les aspects principaux de la gestion de la sécurité des applications et de se familiariser avec les principes, méthodes, procédures et techniques appliquées au sujet du ASMS 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 27034 pour la mise en œuvre et les opérations d'un ASMS . 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 ASMS 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 des applications.

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 ASMS dans une organisation
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de Sécurité des applications
- Membres d'une équipe projet en sécurité des applications
- Opérateurs en technologie des applications
- Membre du personnel d'une organisation voulant se préparer pour un poste en sécurité des applications

Objectifs

- Comprendre les principes de la sécurité des applications et sa mise en œuvre
- Acquérir la terminologie et les connaissances de base nécessaires pour répondre aux exigences de l'ISO 27034 dans le contexte d'une entreprise
- Découvrir les bonnes pratiques de management de la sécurité des applications et son articulation avec la gestion des risques
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 27034 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™

Agenda général

- Le ASMS tel qu'exigé par la norme ISO/CEI 27034 - 7h
- Fonctionnement du ASMS+ Outils de gestion d'un ASMS- 7h
- Examen ISO 27034 Foundation (1h – 50 questions QCM)

L'examen « ISO 27034 Foundation », composé d'un total de 50 questions à choix multiple et d'une durée totale de 1 heure, à livre fermé, atteste du fait que le candidat dispose des connaissances et aptitudes pour comprendre les enjeux liés à un ASMS ainsi que les termes et conditions de son mise en œuvre, de son exécution, de sa surveillance et de son amélioration continue en fonction des exigences de la norme ISO/CEI 27034.

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISO 27034 Practitioner (21 heures)
- ISO 27034 Auditor (21 heures)

Ils peuvent être suivi consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 200 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

Le ASMS tel qu'exigé par la norme ISO/CEI 27034 - 7h

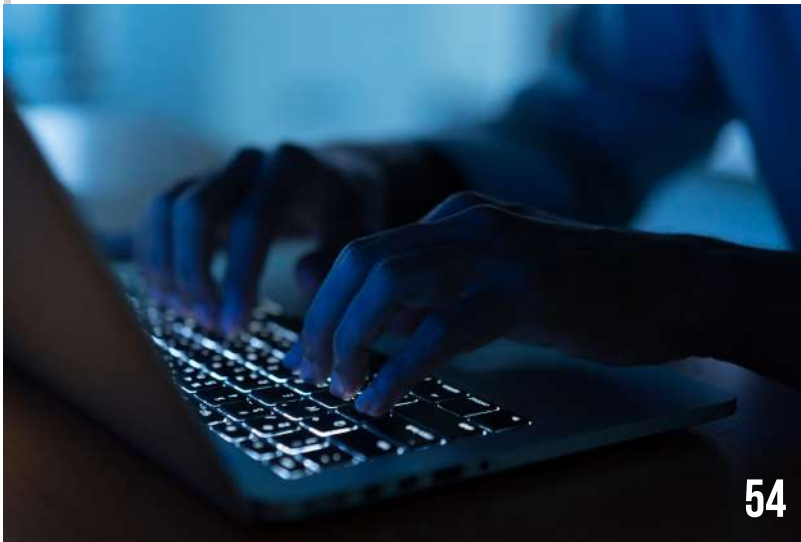
- Système de Management de la sécurité des applications – concepts de base
- Principes fondamentaux de la sécurité des applications
- Les clauses de l'ISO 27034 et l'Annexe A d'ISO 27034
- Le contexte du ASMS au sein de l'entreprise et son champ d'application
- Aspects de leadership et engagement managérial
- Planification d'un ASMS (gestion des risques, mesures de sécurité, applicabilité, etc.)
- Support des opérations d'un ASMS (documentation, ressources, etc.)

Fonctionnement du ASMS - 7H

- Gestion des opérations d'un SMSA
- Surveillance du ASMS (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 27034
- Présentation de la documentation nécessaire aux opérations du ASMS (toolbox)

Examen certifiant « ISO 27034 Foundation »

- 1h, 50 questions QCM à livre fermé)



ISO 27034 Practitioner

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la mise en œuvre d'un programme de gestion de la sécurité des applications et de se préparer par la pratique à mener un projet de mise en œuvre d'un ASMS sur la base de la norme ISO/CEI 27034 selon une méthode éprouvée. Au cours de cette formation, l'étudiant acquerra les bases de connaissance et les aptitudes l'autorisant à identifier, analyser, évaluer et traiter les risques liés à la sécurité des applications dans le respect des exigences de l'ISO 27034 et de 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 des applications 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 ASMS dans une organisation
- Dirigeants d'une entreprise souhaitant se familiariser avec les aspects de Sécurité des applications
- Membres d'une équipe projet en sécurité des applications
- Opérateurs en technologie des applications
- Membre du personnel d'une organisation voulant se préparer pour un poste en sécurité des applications

Objectifs

- Maîtriser les concepts, approches, normes, méthodes et techniques pour participer à la mise en œuvre et la gestion d'un programme de sécurité des applications conforme aux meilleures pratiques au sein d'une organisation selon ISO 27034.
- Comprendre le but, le contenu et la corrélation entre la Sécurité des applications avec d'autres normes et standards de l'industrie
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques de gestion de la sécurité des applications.
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 27034 Practitioner.

Prérequis

Des connaissances minimales sur la sécurité des applications et des concepts connexes sont nécessaires pour la réussite du cours.

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™

Agenda général

- La gestion de la sécurité des applications selon la norme ISO/CEI 27034 - 7h
- La mise en œuvre des techniques de la sécurité des applications sur la base de la norme ISO/CEI 27034 - 7h
- Outils de gestion d'un ASMS dans le cadre d'une organisation - 7h
- Examen ISO 27034 Practitioner (2h – 100 questions QCM)

L'examen « ISO 27034 Practitioner», composé d'un total de 100 questions à choix multiple et d'une durée totale de 2 heures, à livre fermé, atteste du fait que le candidat dispose des connaissances et aptitudes pour comprendre les enjeux liés à un SMSA ainsi que les termes et conditions de son mise en œuvre, de son exécution, de sa surveillance et de son amélioration continue en fonction des exigences de la norme ISO/CEI 27034.

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISO 27034 Lead Auditor (21 heures)

Ils peuvent être suivi consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.
Le support de cours officiel (composé de plus de 500 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

- La gestion de la sécurité des applications selon la norme ISO/CEI 27034 - 7h
- La mise en œuvre des techniques de la sécurité des applications sur la base de la norme ISO/CEI 27034 - 7h
- Outils de gestion d'un ASMS dans le cadre d'une organisation - 7h
- Examen ISO 27034 Practitioner (2h – 100 questions QCM)

ISO 27034 Auditor

Cette formation de 21 heures offre aux participants l'occasion de monter en compétence sur la fonction d'assurance de la gestion de la sécurité des applications 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, l'étudiant 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 ASMS 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

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

Objectifs

- Comprendre les principes de fonctionnement d'un ASMS selon ISO 27034
- Développer les aptitudes nécessaires pour mener à bien un audit ISO 27034 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 ASMS
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 27034 Auditor.

Prérequis

Des connaissances minimales sur la sécurité des applications et des concepts connexes sont nécessaires pour la réussite du cours.

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™

Agenda général

- Planifier et mettre en œuvre un audit de ASMS– 7 heures
- Mener un audit de ASMS– 7 heures
- Clôturer et assurer le suivi d'un audit de ASMS + Exercices préparatoires supplémentaires (QCM & questions ouvertes) – 7 heures
- Examen ISMS Auditor (2 heures – 100 questions QCM)

L'examen « ISO 27034 Lead Auditor», composé d'un total de 100 questions à choix multiple et d'une durée totale de 2 heures, à livre fermé, atteste du fait que le candidat dispose des connaissances et aptitudes pour comprendre les enjeux liés à un SMSA ainsi que les termes et conditions de son mise en œuvre, de son exécution, de sa surveillance et de son amélioration continue en fonction des exigences de la norme ISO/CEI 27034.

Cette formation peut se combiner avec d'autres modules distincts comme :

- ISO 27034 practitioner (21 heures)

Ils peuvent être suivi consécutivement à cette formation de base ou combinés avec d'autres modules de notre catalogue.

Le support de cours officiel (composé de plus de 300 pages de contenus, d'exercices préparatoires à l'examen) ainsi que l'ensemble du matériel pédagogique de soutien (exemples de livrables, méthodes, etc.) sont fournis sous licence Creative Commons par CERTI-TRUST™.

Programme détaillé

Planifier et mettre en œuvre un audit de ASMS -- 7H

- Concepts de base, principes et critères d'audit selon ISO 19011
- Déroulement général d'un audit de AsMS
- 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 ASMS – 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 ASMS (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 ISO 27034 lead auditor (2h – 100 questions QCM)

Contactez-Nous !

Addresse

27, Place de la Madeleine, F-75008
Paris (France)

Numéro de téléphone

+33 (0)7 61 56 58 37

Email

sales.france@certi-trust.com

Certi-Trust

Certi-Trust

Certi-Trust

@certitrust

@certi_Trust

www.certi-trust.com


CERTITRUST
LEARNING IN THE DIGITAL ERA