Document mis à jour en mai 2025

CATALOGUE DES FORMATIONS

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

formind ACADEMY

SOMMAIRE

SOMMAIRE

SOMMAIRE

BIENVENUE À LA FORMIND ACADEMY

Formind est un cabinet de conseil et d'intégration en Cybersécurité, créé en 2010, dont la mission est simple et belle : protéger ses clients. Nous sommes près de 200 experts, passionnés, animés par des valeurs de rigueur, d'exigence, de partage et d'écoute.

Nous sommes ravis de partager nos connaissances et notre expérience en créant Formind Academy, centre de formation Cybersécurité. Nos formateurs sont enthousiastes, passionnés, expérimentés, certifiés et accrédités !

Avec Formind Academy, nous nous engageons :

RIEN QUE LA CYBERSÉCURITÉ, TOUTE LA CYBERSÉCURITÉ

Tout le monde est concerné ! Ce qui est passionnant avec la cybersécurité, c'est que vous travaillez avec tous les métiers. C'est pour ça que nous proposons une offre complète : de la gouvernance pour la direction et les managers, du juridique pour la protection des données personnelles, et de la technique pour les administrateurs et les spécialistes.

LE PARFAIT DOSAGE ENTRE THÉORIE ET RETOURS D'EXPÉRIENCES PRATIQUES

Halte aux cours standards et insipides ! Bien que nous dispensions des formations certifiantes, nous enrichissons les contenus de nos cours par nos propres études de cas et de nos retours d'expérience. Nous pouvons aller jusqu'à la création d'un cours ex nihilo, 100% adapté à vos besoins spécifiques. Nous comptons de très nombreuses références client.

DES FORMATEURS DE TRÈS HAUT NIVEAU

Ne comptez-pas sur nous pour lire les diapo Powerpoint en cours ! Nos formateurs sont certifiés (ils ont passé le même examen que vous) et accrédités (ils ont été audités et ont obtenu l'autorisation d'enseigner un cours). Leurs capacités pédagogiques sont validées, ainsi que leur maîtrise du contenu et leur capacité à illustrer chaque point par des anecdotes et des exemples réels.

UNE EXPÉRIENCE STIMULANTE

Nos experts parlent à vos experts ! Nous proposons des formations avant-gardistes, surtout en cyber sécurité, où tout retard se paie très cher, ainsi qu'une pédagogie innovante en s'appuyant par exemple sur la réalité Virtuelle. Nos formateurs sont formés aux techniques pédagogiques (inductive, déductive, interactive), pour favoriser la transmission des connaissances et des compétences.
Et nos salles sont très agréables : vous apprécierez nos canapés Chesterfield !

Nous animons des formations partout en France, dans nos locaux ou bien les vôtres !

A bientôt,

Hervé Morizot, Associé

POURQUOI FORMIND ACADEMY ?

Formind Consulting dispose de son propre centre de formation : Formind Academy. L'objectif est double :

- **Former nos propres équipes.** Chez Formind, la formation est essentielle car elle permet à nos équipes d'être toujours à jour, aussi bien sur les techniques ou les produits d'éditeurs, les aspects juridiques que sur les aspects de gouvernance des systèmes d'information.
- **Former vos équipes** ! Nous disposons d'un catalogue très riche de formations en cybersécurité.
  - Nous proposons des formations certifiantes (PECB, ISC2, Isaca), ainsi que des formations sur mesure, complètement adaptées à vos besoins.
  - Notre catalogue compte une soixantaine de références de formation en sécurité de l'information.
  - Nous pouvons inscrire vos collaborateurs dans nos sessions ouvertes à tous, ou bien organiser un cours selon vos disponibilités, en France ou à l'étranger, en français ou en anglais.
  - Nos formateurs sont certifiés (ils ont passé le même examen que vous) et accrédités (ils ont été audités et ont le droit d'enseigner).
  - Nos salles de cours sont accueillantes. Nous avons mis l'accent sur la décoration des salles, chaleureuses et confortables.

95%

des brèches de cybersécurité sont liées à une erreur humaine

Source : Gartner. Why Cloud Security Is Everyone's Business - Smarter With Gartner

80%

des entreprises dans le monde ont été victime de phishing

Source : Baromètre Cesin 6ème édition du baromètre annuel du CESIN - CESIN

60%

La gouvernance est le premier enjeu de demain (60%), suivi par celui de la formation et de la sensibilisation des utilisateurs (56%).

Source : EC Council - 2020

214 jours

en moyenne pour réaliser qu'un malware infecte un système d'information d'entreprise, et 77 jours sont nécessaires pour se remettre complètement d'une attaque informatique

NOTRE OFFRE DE FORMATION

SENSIBILISATION

- Changer les comportements
- Quelques heures

FONDAMENTAUX

- Acquérir les connaissances de base
- 1 ou 2 jours

EXPERT

- Acquérir des compétences
- 3 à 5 jours

NOS ATOUTS

Des formateurs certifiés ET accrédités (audités et autorisés à enseigner)

Nous sommes spécialisés dans la cybersécurité et nous ne nous éparpillons pas !

Des cours enrichis par nos études de cas et expériences terrain

D'une offre standard certifiante à des cours 100% sur mesure

100% de réussite, aux examens sur l'ensemble de nos équipes que nous avons formées (60 candidats en 2020)

Des partenariats avec les leaders : PECB, (ISC)2, Isaca, etc.

NOTRE APPROCHE : UNE DÉMARCHE 100% QUALITÉ

La qualité dans l'analyse et anticipation du besoin

- la bonne formation au bon moment pour répondre aux besoins de l'organisation
- connaître, écouter, comprendre le client
- formuler de manière explicite

La qualité dans la conception

- l'équilibre entre la créativité et les compétences organisationnelles et techniques
- définir les spécifications et spécificités de la formation
- définir et choisir la solution pédagogique : format, workhops, Réalité Virtuelle, etc.

La qualité dans la réalisation

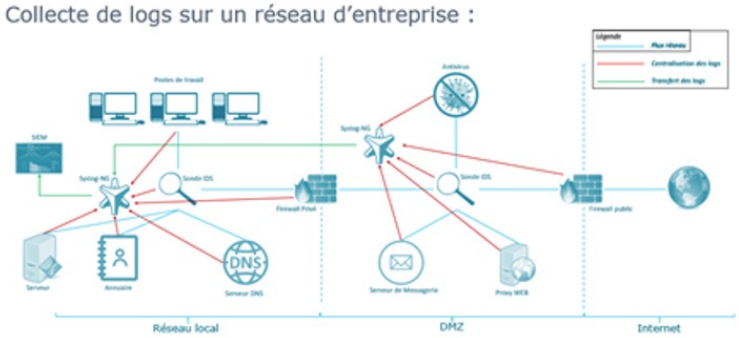
- la maîtrise du contenu et des outils, les retours d'expérience du formateur, son savoir-faire pédagogique
- la performance de la formation
- la maîtrise des coûts et des délais

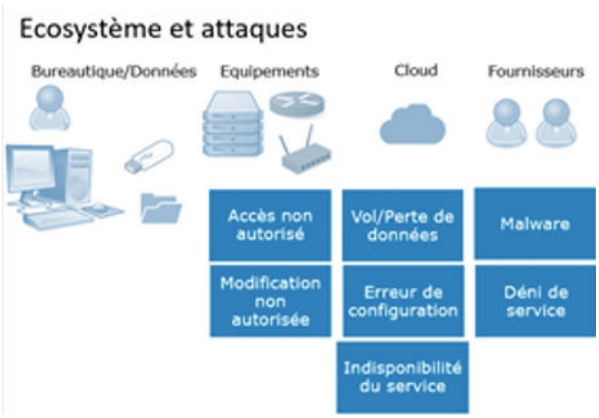
La qualité du feed-back

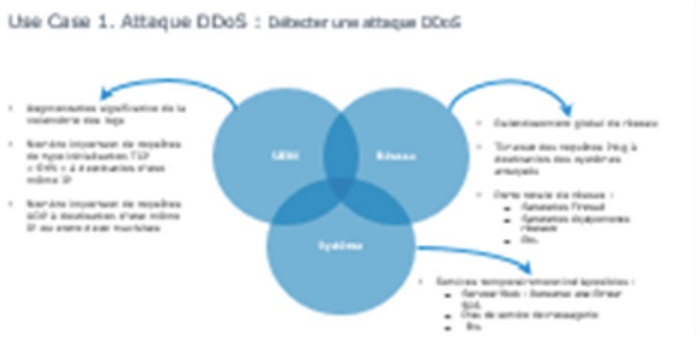
- service et création de valeur pour l'apprenant
- l'accompagnement , la maintenance et le suivi post formation
- l'épanouissement personnel et professionnel

EXEMPLES DE SUPPORTS

Les stagiaires disposent de supports afin de suivre les présentations, démonstrations, TP, TD et études de cas. Les supports présentent les notions, les démarches, de façon synthétiques et accompagnés de schémas permettant d'avoir une vue de l'ensemble des notions abordées en animation.





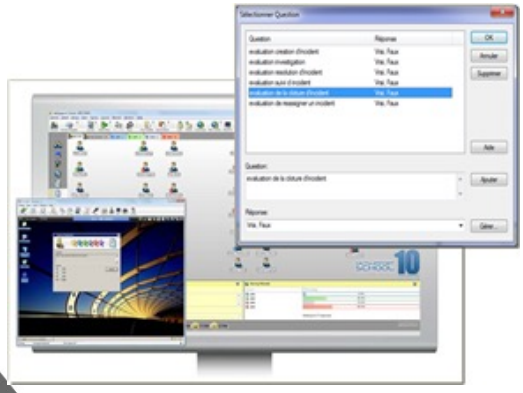


Le pilotage de la qualité

Le pilotage de la qualité s'effectue en 2 temps : l'évaluation à chaud puis à froid. La première relève d'un bilan général, du point de vue sur les évaluations, des remarques sur les moyens mis en œuvre et enfin des suggestions d'amélioration. La seconde vise à évaluer la qualité de l'animation et des supports, l'organisation et les moyens et enfin l'apport de la formation.

Plus particulièrement, l'évaluation à chaud valide l'acquis des connaissances tout au long de la session sur la base d'un questionnaire en ligne personnel :

- En s'appuyant sur le Module de création de QCM d'évaluations d'un outil tel que Net Support School
- Collecte automatique des travaux réalisés par les stagiaires
- A chaque fin de module, l'animateur vérifie que les manipulations ont correctement générées les résultats attendus dans le dossier stagiaire de chaque poste



L'évaluation à froid prend la forme d'un questionnaire envoyé au stagiaire une semaine après avoir commencé à utiliser les connaissances abordées en formation :

- Pour chaque fonction présentée en stage, un QCM sous forme d'images est proposé au stagiaire
- Le principe : retrouver les fonctionnalités, démarches, notions abordées durant la session

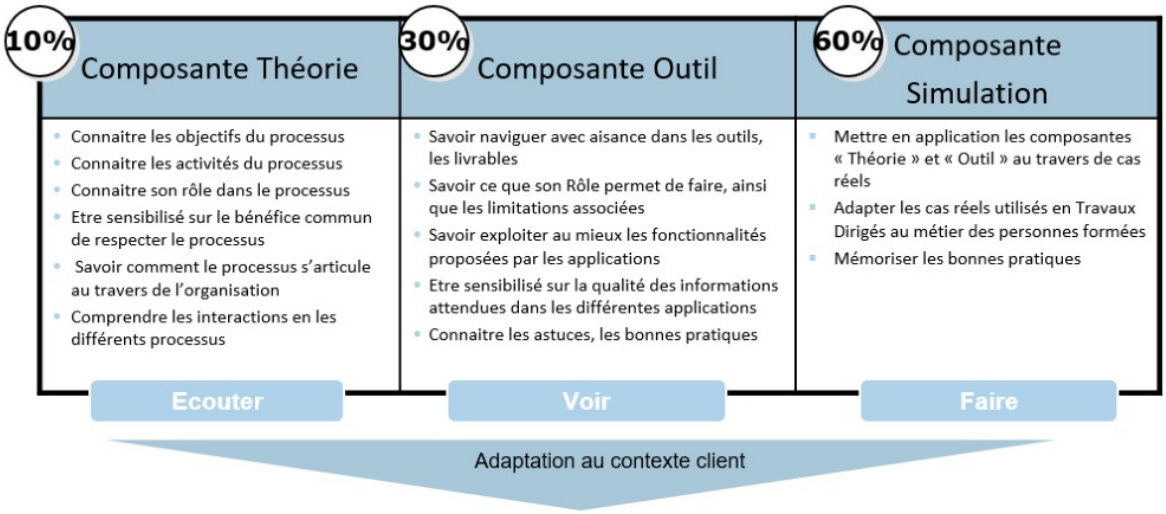
Pour chaque fin de session, **une évaluation à chaud est réalisée** afin de recueillir les éléments de qualité et d'amélioration de la prestation pour les sessions suivantes :

Evaluation de la session par le stagiaire

Evaluation de la session par le formateur

NOTRE APPROCHE PÉDAGOGIQUE

La journée se découpe en 3 temps avec 3 objectifs distincts :



Support de cours formateur

Support à disposition sur clé USB et document imprimé :
- Support identique au stagiaire plus des annotations sur les questions réponses, le timing, les recommandations d'animation

Support stagiaire *(remis en début de session)*

Support à disposition sur clé USB et document imprimé :
- Vidéos de démonstration de chacune des fonctions
- Support complet de la journée

Cahier exercice avec corrigé *(remis en fin de session)*

Support à disposition sur clé USB et document imprimé :
- Vidéos de démonstration de chacun des exercices
- Support de chacun des exercices avec les corrections

Aide mémoire *(remis en début de session)*

Support à disposition sur clé USB et document imprimé :
- Rappel des principales fonctionnalités
- Lexique

NOTRE MÉTHODOLOGIE PÉDAGOGIQUE

Au sein de FORMIND ACADEMY, l'apprenant est le cœur du système. Notre centre de formation propose une démarche inductive à travers laquelle l'apprenant participe activement à des mises en situation, et à des démonstrations animées par des formateurs accrédités.

Nos formateurs sont formés aux techniques pédagogiques (inductive, déductive, interactive), pour favoriser la transmission des connaissances et des compétences. Cette méthodologie positionne l'apprenant dans une pédagogie participative et collaborative. Nous nous appuyons sur des exposés théoriques, des exercices pratiques, l'application des concepts au sein de logiciels du marché, ou des matrices de type Excel. Nous créons également nos propres méthodes et outils pédagogiques lors de formations sur mesure (workshops, Capture the Flag, etc.)

Modalités et délais d'accès

L'accès à nos formations peut été initié, soit par l'employeur, soit à l'initiative du salarié avec l'accord de ce dernier, soit à l'initiative propre du salarié.

- Pour chaque demande de formation, notre service réalise sous 8 j un entretien téléphonique afin d'établir une formation personnalisée qui prend en compte les attentes, les préférences et les contraintes du prospect. Une politique de prévention de la violence dans leur(s) établissement(s) peut-être également proposée. Lors de cet entretien, les modalités de déroulement et de sanction de la formation, le ou les objectifs, les connaissances et les compétences acquises, les sources de financement, etc..., sont précisés.
- Une proposition commerciale (hors subrogation OPCO) est transmise sous 8 j, un programme adapté ainsi qu'une fiche client, qui permet de faciliter les échanges administratifs.
- A réception du devis signé l'organisation logistique, technique, pédagogique et financière est établie lors des divers échanges avec notre service formation et le commanditaire. Le devis est valable 30 j.
- Le délai d'accès aux formations, tient compte de ces différentes formalités afin d'être accessible dans un temps minimum d'un mois avant le début de l'action.

Modalité d'accès pour les PSH

Modalité d'accès pour les personnes en situation de handicap (PSH) .

Nous veillons au respect des conditions d'accueil des Publics concernés et étudions au cas par cas toutes les situations de handicap afin d'envisager une intégration dans la formation. Si vous êtes en situation de handicap, nous trouverons des solutions pour vous accueillir. Nos formations peuvent être adaptées aux différentes situations de handicap (cf. procédure d'accueil des personnes en situation de handicap). Nous sommes à votre disposition pour étudier les adaptations nécessaires à votre besoin.
Merci de nous écrire à formation@formind.fr

Contact Référent handicap :
Elsa Gressinger
elsa.gressinger@formind.fr

NOTRE MÉTHODOLOGIE D'EVALUATION

1. Avant la formation

Tout d'abord, avant même d'entamer le processus de formation, il s'agit d'évaluer vos besoins spécifiques. D'ailleurs, les entretiens annuels ou entretiens professionnels (qui eux ont lieu tous les deux ans) aideront à mettre en avant vos besoins prioritaires.

Ensuite une évaluation des prérequis est effectuée dans le but d'avoir à l'esprit sa marge de progrès et ainsi faciliter la mesure du chemin parcouru avant et après la formation.

Pour ce faire, rien de plus efficace qu'un test de connaissances en amont ou bien un entretien avec le formateur.

2. Pendant la formation

Tout au long de la formation et ce, quelle qu'en soit la durée, le formateur valide la compréhension de même que l'acquisition de vos connaissances. La plupart des formateurs utilisent dans ce contexte des tests ou des jeux de mise en situation. Ils confirment donc, la compréhension et facilitent la mémorisation de l'apprentissage sur le long terme.

3. A l'issue de la formation

A la fin de chaque formation, il est crucial de prévoir un outil de mesure de la satisfaction des participants sur tous les éléments du dispositif tels que le contenu, la méthode du formateur, ses compétences pédagogiques, l'organisation du cursus…

En effet, ce retour d'expérience peut être fait de façon orale, en prévoyant un tour de table par exemple, ou bien de façon individuelle et écrite, notamment en distribuant des questionnaires en fin de formation).

Les outils les plus fréquemment utilisés restent les quizz, les questionnaires vrai-faux, ou encore les questionnaires d'auto-évaluation avant-après.

4. Quelques mois après avoir terminé la formation

Trois à six mois après la formation, il est nécessaire de mesurer son impact en situation professionnelle de l'apprenant. On parle d'évaluation à froid.

Plusieurs méthodes peuvent être utilisées pour évaluer cette étape :

- Une grille d'analyse de l'évolution des comportements à la suite de la formation
- Une analyse de l'évolution des objectifs individuels
- De l'efficacité et de l'efficience du salarié à son poste
- Une analyse de l'évolution des indicateurs de performance.

NOTRE DÉMARCHE DE CONCEPTION D'UNE FORMATION PERSONNALISÉE

ANALYSE

Analyse en besoin de montées en compétences

Définition des profils et matrices de compétences

Proposition d'accompagnement et de planning

CONSTRUCTION / ADAPTATION DU CONTENU

Atelier de travail

Construction des supports

Adaptation des messages

SESSIONS DE FORMATION

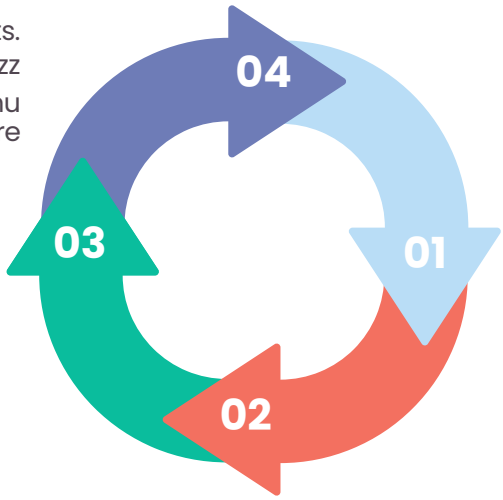
Animation des sessions de formation

CONTRÔLE

Suivi des retours des participants.

Suivi des résultats aux quizz

Nouvelles adaptations du contenu si nécessaire



SÉCURITÉ DE L'INFORMATION

- **Prise de poste RSSI & manager cyber sécurité**
- **ISO 27001** : sécurité de l'information
- **ISO 27005** : gestion des risques liés à la sécurité de l'information
- **Ebios** : méthodes d'appréciation des risques
- **ISO 27035** : Gestion des incidents

Manager Cyber sécurité – ISO 27032 1/2

Durée : 5 jours

Langue : FR

Examen inclu

Pré requis

- Avoir suivi la formation gouvernance SSI ou avoir les connaissances équivalentes

POUR QUI

- RSSI en poste ou sur le point de prendre cette fonction
- Consultants désirant assister au quotidien un RSSI
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Responsables du développement d'un programme de cybersécurité

OBJECTIFS PÉDAGOGIQUES

- RSSI en poste ou sur le point de prendre cette fonction
- Consultants désirant assister au quotidien un RSSI
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Responsables du développement d'un programme de cybersécurité

Programme

Jour 1: Introduction à la cybersécurité et aux concepts connexes, tels que définis par l'ISO/IEC 27032

Jour 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaques

Jour 3 : Contrôles en cybersécurité, partage des informations et coordination

Jour 4: Gestion des incidents, suivi et amélioration continue

Jour 5 :

révision

examen

Examen

Durée : 3 heures

Type d'examen: QCM

Note de passage : 70%

Langue : Anglais, français

PROGRAMME & CERTIFICATION

Jour 1: Introduction à la cybersécurité et aux concepts connexes, tels que définis par l'ISO/IEC 27032
Jour 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaque
Jour 3 : Contrôles en cybersécurité, partage des informations et coordination
Jour 4 : Gestion des incidents, suivi et amélioration continue
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :
Domaine 1 : Principes et concepts fondamentaux de la cybersécurité
Domaine 2 : Rôles et responsabilités des parties prenantes
Domaine 3 : Gestion des risques liés à la cybersécurité
Domaine 4 : Mécanismes d'attaque et contrôles en cybersécurité
Domaine 5 : Partage de l'information et coordination
Domaine 6 : Intégrer le programme de cybersécurité dans le management de la continuité des activités
Domaine 7 : Gestion des incidents de cybersécurité et mesure de la performance

Durée : 3 heures

QCM

Note de passage : 70%

Langue : Anglais, français

Prérequis: Une expérience de 2 ans en cyber sécurité est préconisée.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants.
- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Exercices pratiques basés sur une étude de cas incluant des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG.

ISO 27001 Lead Implementor – Sécurité de l'Information 1/2

Niveau : Expert

Durée : 5 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

Eligible au FNE, moncompteformation.gouv.fr : code 236611

RÉSUMÉ

La formation ***ISO/CEI 27001 Lead Implementer*** permet d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la sécurité de l'information pour sécuriser les informations sensibles, améliorer l'efficacité et la performance globale de l'organisation.

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de **PECB Certified ISO/CEI 27001 Lead Implementer.** En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

POUR QUI

- Experts de la sécurité de l'information et de l'audit
- Tous les professionnels qui évaluent, conçoivent, déploient, supervisent et optimisent la sécurité de l'information avec les mesures de sécurité associées
- DSI, RSI, RSSI, Chief Digital Officier
- Consultants Auditeurs IT / IS, tous professionnels du contrôle, de l'assurance, de la gestion des risques et de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
2. Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
3. Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
4. Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
5. Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information
6. Préparer l'examen ISO 27001 LI

PROGRAMME & CERTIFICATION

Jour 1 : Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI
Jour 2 : Planification de la mise en œuvre d'un SMSI
Jour 3 : Mise en œuvre d'un SMSI
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :
Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
Domaine 2 : Système de management de la sécurité de l'information
Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001
Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001
Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001
Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001
Domaine 7 : Préparation de l'audit de certification d'un SMSI

Durée :	Type d'examen:	Note de passage :	Langue :
3 heures	QCM	70%	Anglais, français

Prérequis: Une bonne connaissance de la norme ISO/CEI 27001 et des principes de mise en œuvre.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants
- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Exercices pratiques basés sur une étude de cas incluant des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

ISO 27001 Lead Auditor – Sécurité de l'Information 1/2

Niveau : Expert

Durée : 5 jours, examen à passer à la suite de la formation

Certification : PECB Certified ISO/IEC 27701 Lead Auditor

Eligible au FNE, moncompteformation.gouv.fr : code 235823

RÉSUMÉ

Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1. À l'aide d'exercices pratiques, vous serez en mesure d'acquérir des connaissances sur la protection de la vie privée dans le contexte du traitement des informations d'identification personnelle (IIP), et de maîtriser des techniques d'audit afin de devenir compétent pour gérer un programme et une équipe d'audit, communiquer avec des clients et résoudre des conflits potentiels.
Après avoir maîtrisé les concepts d'audit démontrés et réussi l'examen, vous pourrez demander la certification ***PECB Certified ISO/IEC 27001 Lead Auditor***. Cette certification, reconnue à l'échelle internationale, démontre que vous possédez l'expertise et les compétences nécessaires pour auditer des organismes basés sur les bonnes pratiques.

POUR QUI

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la sécurité de l'information
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Experts techniques désirant préparer un audit du Système de management de la sécurité de l'information
- Conseillers spécialisés en management de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001
2. Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
3. Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
4. Savoir diriger un audit et une équipe d'audit, interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
5. Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011
6. Préparer l'examen ISO 27001 LA

PROGRAMME & CERTIFICATION

Jour 1 : Introduction au Système de management de la sécurité de l'information et à la norme ISO/CEI 27001
Jour 2 : Principes, préparation et déclenchement de l'audit
Jour 3 : Activités d'audit sur site
Jour 4 : Clôture de l'audit
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :
Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
Domaine 2 : Système de management de la sécurité de l'information (SMSI)
Domaine 3 : Principes et concepts fondamentaux de l'audit
Domaine 4 : Préparation d'un audit ISO/CEI 27001
Domaine 5 : Réalisation d'un audit ISO/CEI 27001
Domaine 6 : Clôturer un audit ISO/CEI 27001
Domaine 7 : Gérer un programme d'audit ISO/CEI 27001

Durée : 3 heures	Type d'examen : QCM	Note de passage : 70%	Langue : Anglais, français

Prérequis: Une bonne connaissance de la norme ISO/CEI 27001 et dans les principes de l'audit.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants.
- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Exercices pratiques basés sur une étude de cas incluant des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG.

ISO 27005 Risk Manager – Risques liés à la sécurité de l'information 1/2[21]

Niveau : Expert

Durée : 3 jours

Certification : Oui

Eligible au FNE, moncompteformation.gouv.fr : code 235635

RÉSUMÉ

La formation ***ISO/IEC 27005 Risk Manager*** permet de développer les compétences nécessaires pour maîtriser les processus de management du risque liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. Au cours de cette formation, vous acquerrez également une compréhension approfondie des bonnes pratiques des méthodes d'évaluation des risques telles qu'OCTAVE, EBIOS, MEHARI et la TRA harmonisée. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre du SMSI présenté dans la norme ISO/IEC 27001.

POUR QUI

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans un organisme
- Consultants de l'IT
- Professionnels de l'IT
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de management du risque
- Agents de la sécurité de l'information
- Agents de la protection de la vie privée

OBJECTIFS PÉDAGOGIQUES

1. Acquérir les connaissances nécessaires à la réussite de l'examen CRISC
2. Maîtriser les concepts de la gestion de la sécurité de l'information
3. Évaluer, concevoir, déployer, superviser et améliorer tout système de gestion de la sécurité de l'information, aux plans organisationnels et techniques
4. Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information et matière de gestion de la sécurité
5. Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en gestion de la sécurité de l'information et en audit sur cette thématique

ISO 27005 Risk Manager – Risques liés à la sécurité de l'information 2/2 [22]

PROGRAMME & CERTIFICATION

Introduction au Certified in Risk and Information Systems Control
Domaine 1 : identification des risques informatiques
Domaine 2 : évaluation des risques informatiques
Domaine 3 : réponse et atténuation des risques
Domaine 4 : surveillance et déclaration des contrôles et des risques
Préparation à l'examen

L'examen PECB Certified Human Resources Security Foundation dure une heure. Il couvre les domaines suivants :
Domaine 1 : identification des risques informatiques (27 %)
Domaine 2 : évaluation des risques informatiques (28 %)
Domaine 3 : réponse et atténuation des risques (23 %)
Domaine 4 : surveillance et déclaration des contrôles et des risques (22 %)

Durée de l'examen:	Type d'examen :	Note de passage :	Langue :
3 heures	Etude de cas	70%	Anglais, français

Prérequis: Il est recommandé que les candidats disposent d'au moins trois (3) ans d'expérience dans la gestion des risques IT et du contrôle IS. Des certifications professionnelles en gestion de la sécurité et des risques, en audit, en gestion de projet et de de services sont les bienvenues.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants
- Un manuel de cours
- Les livres officiels de l'ISACA, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés par l'ISACA.

EBIOS RM – Méthode d'appréciation des risques 1/2

Niveau : Expert

Durée : 3 jours

Certification : oui

Formation éligible FNE , moncompteformation.gouv.fr : code FNE 236760

RÉSUMÉ

La formation ***EBIOS*** permet d'acquérir les connaissances et développer les compétences nécessaires pour maîtriser les concepts et les éléments de management des risques liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la méthode EBIOS.

Grâce aux exercices pratiques et aux études de cas, vous acquerrez les connaissances et les compétences nécessaires pour réaliser une appréciation optimale des risques liés à la sécurité de l'information et pour gérer les risques dans les temps par la connaissance de leur cycle de vie. Cette formation s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/CEI 27001.

POUR QUI

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnel participant aux activités d'appréciation des risques selon la méthode EBIOS
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode EBIOS

OBJECTIFS PÉDAGOGIQUES

1. Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
2. Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
3. Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
4. Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme
5. Acquérir les compétences nécessaires afin de mener une étude EBIOS
6. Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS

CERTIFICATION

L'examen PECB Certified EBIOS Risk Manager remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

Domaine 1 : Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information selon la méthode EBIOS
Domaine 2 : Programme de gestion des risques liés à la sécurité de l'information basé sur EBIOS
Domaine 3 : Appréciation des risques liés à la sécurité de l'information basée sur la méthode EBIOS

Prérequis: Une connaissance en gestion du risque est recommandée.

MATERIEL

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants
- Un manuel de cours contenant plus de 350 pages d'informations et d'exemples pratiques est fourni
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont **inclus** dans le prix de l'examen
- À l'issue de la formation, un **certificat de participation de 21 crédits DPC** (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

ISO 27035 Lead Security Incident Manager 1/2

Niveau : Expert

Durée : 5 jours, examen inclus

Certification : PECB Certified ISO/CEI 27035 Lead Incident Manager

Eligible au FNE, moncompteformation.gouv.fr : code 236723

RÉSUMÉ

La formation ***ISO/CEI 27035 Lead Incident Manager*** permet d'acquérir l'expertise nécessaire pour accompagner une organisation lors de la mise en œuvre d'un plan de gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035. Durant cette formation, vous acquerrez une connaissance approfondie sur le modèle de processus permettant de concevoir et de développer un plan de gestion des incidents des organisations. La compatibilité de cette formation avec l'ISO/CEI 27035 prend également en charge l'ISO/CEI 27001 en offrant des lignes directrices pour la gestion des incidents de sécurité de l'information.

Après avoir maîtrisé l'ensemble des concepts relatifs à la gestion des incidents de sécurité de l'information vous pouvez vous présenter à l'examen et postuler au titre de ***PECB Certified ISO/CEI 27035 Lead Incident Manager***. En étant titulaire d'une certification Lead Incident Manager de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles nécessaires pour soutenir et diriger une équipe dans la gestion des incidents de sécurité de l'information.

POUR QUI

- Gestionnaires des incidents de sécurité de l'information
- Responsables des TIC
- Auditeurs des technologies de l'information
- Responsables souhaitant mettre en place une équipe de réponse aux incidents
- Responsables souhaitant apprendre davantage sur le fonctionnement efficace d'une équipe de réponse aux incidents
- Responsables des risques liés à la sécurité de l'information
- Administrateurs professionnels des systèmes informatiques
- Administrateurs professionnels de réseau informatique
- Membres de l'équipe de réponse aux incidents
- Personnes responsables de la sécurité de l'information au sein d'une organisation

OBJECTIFS PÉDAGOGIQUES

1. Maîtriser les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/CEI 27035
2. Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres réglementaires
3. Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en œuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information
4. Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
5. Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
6. Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

PROGRAMME & CERTIFICATION

Jour 1 : Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035
Jour 2 : Conception et préparation d'un plan de gestion des incidents de sécurité de l'information
Jour 3 : Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information
Jour 4 : Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :

- **Domaine 1 :** Principes et concepts fondamentaux relatifs à la gestion des incidents liés à la sécurité de l'information
- **Domaine 2 :** Meilleures pratiques de la gestion des incidents liés à la sécurité de l'information selon la norme ISO/CEI 27035
- **Domaine 3 :** Conception et développement d'un processus de gestion des incidents organisationnels selon l'ISO/CEI 27035
- **Domaine 4 :** Préparation aux incidents de sécurité de l'information et mise en œuvre d'un plan de gestion des incidents
- **Domaine 5 :** Lancement du processus de gestion des incidents et traitement des incidents liés à la sécurité de l'information
- **Domaine 6 :** Surveillance et mesure de la performance
- **Domaine 7 :** Améliorer les processus et les activités de gestion des incidents

Durée de l'examen: 3 heures	Type d'examen : Etude de cas	Note de passage : 70%	Langue : Anglais, français

Prérequis: une compréhension fondamentale de l'ISO / CEI 27035 et des connaissances approfondies sur la sécurité de l'information sont nécessaires..

MATERIEL & INGENIERIE PEDAGOGIQUE

- Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants
- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Exercices pratiques basés sur une étude de cas incluant des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG.

CYBERSÉCURITÉ

- Sécurité des réseaux
- Identité numérique et PKI
- Sécurité Applicative
- EDR/XDR/NDR

Sécurité des réseaux

Niveau : Expert

Durée : 3 jours

Prérequis: Connaissance de base d'un système Linux et Windows
Connaissance des réseaux et modèle OSI

RÉSUMÉ

Ce cours a pour sujet les spécifications de la sécurité réseaux en termes de détections de vulnérabilités et les réponses administrateurs appropriées à travers différents ateliers.

POUR QUI

- Administrateur
- Architecte
- Chef de projet
- Toute population travaillant dans l'informatique

OBJECTIFS PÉDAGOGIQUES

1. Comprendre les enjeux et les principes essentiels en matière de la sécurité
2. Comprendre les grandes catégories de menaces pesant sur les réseaux (usurpation d'identité, interception, déni de service,...)
3. Connaitre les différentes étapes d'une intrusion dans un réseau
4. Savoir identifier quelques vulnérabilités, et comprendre comment les corriger
5. Connaître les bonnes pratiques d'administration au sens sécurité
6. Savoir comment détecter, analyser et réagir à certaines attaques et alerter
7. Apprendre à utiliser quelques outils permettant de réaliser une première analyse.

PROGRAMME

Jour 1 : Introduction sécurité et sécurité des réseaux
Jour 2 : Savoir identifier les vulnérabilités
Jour 3 : Administrer, analyser, détecter et réagir

Aucun prérequis

MATERIEL & INGENIERIE PEDAGOGIQUE

Matériel informatique fourni

Documents supports de formation projetés

INFORMATIONS GÉNÉRALES

- Animation des sessions par des consultants experts en sécurité
- Nombreux Ateliers, chaque participant dispose d'un PC.
- Adaptation des messages en fonction des populations
- Supports de formation variés (Quiz, Démonstrations,)

Identité numérique - PKI

Niveau : Perfectionnement

Durée : 2 jours

Prérequis: Bonnes connaissances en systèmes, réseaux et sécurité informatique

RÉSUMÉ

Ce cours a pour sujet les bases de l'identité numérique, dégageant une vue globale pour différencier les notions liées, et les appliquer par un cas pratique dans une infrastructure à clés publiques et manipulant des certificats.

POUR QUI

- Ingénieurs
- Administrateurs systèmes et réseaux

OBJECTIFS PÉDAGOGIQUES

1. Les stagiaires sont capables de lire l'offre, savent qualifier un besoin.
2. Les stagiaires savent faire la distinction entre identité et fédération
3. Les stagiaires savent faire la distinction entre identification authentification et preuve
4. Les stagiaires savent faire la différence entre identité et gouvernance
5. Les stagiaires connaissent les notions liées aux infrastructures à clef publique.
6. Les stagiaires comprennent et savent implémenter une solution pour délivrer des certificats, révoquer des certificats, gérer des certificats

PROGRAMME

Jour 1

L'identité numérique
Sensibilisation
Concepts fondamentaux de l'identité et l'authentification

Jour 2

Cryptographie
Principe, primitives et pratiques
Certificats et PKI
Principes et fonctionnement, x509, Pratique, OpenSSL, PKI d'entreprise, HSM et cérémonie
Bonnes pratiques sur les PKI
TP : EJBCA

MATERIEL & INGENIERIE PEDAGOGIQUE

Matériel informatique fourni

Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques

INFORMATIONS GÉNÉRALES

Suivi pédagogique personnalisé

Sécurité Applicative

Niveau : Perfectionnement

Durée : 2 jours

RÉSUMÉ

Ce cours a pour sujet la sécurité applicative sous la forme d'une compétition entre stagiaires sur un Bug Bounty pour dégager de manière personnelle les vulnérabilités sur un SI et les expliquer

POUR QUI

- Professionnels IT en charge de la sécurité des systèmes d'information,
- Auditeurs sécurité

OBJECTIFS PÉDAGOGIQUES

- Faire apprendre les vulnérabilités classiques d'applications Web PHP, iOS et Android à travers le jeu
- Apprendre par une approche offensive à exploiter les vulnérabilités
- Apprendre à corriger les vulnérabilités rencontrées
- Stimuler les équipes en les mettant en compétition

PROGRAMME

Jour 1

- Introduction, présentation synthétique des principales vulnérabilités sur les applicatifs Web/Android/iOS
- mise en place du Bug Bounty, présentation des règles du jeu, présentation des outils
- Bug Bounty

Jour 2

- Temps du Bug Bounty avec débriefing par les formateurs à intervalles réguliers sur les vulnérabilités les plus identifiées.
- Présentation des principales vulnérabilités et qui n'auraient pas été identifiées par les stagiaires

Prérequis: Les stagiaires connaissent l'organisation d'un système d'information
Les stagiaires connaissent les notions fondamentales de l'infrastructure d'un SI

MATERIEL & INGENIERIE PEDAGOGIQUE

Tableau des scores finaux par équipe

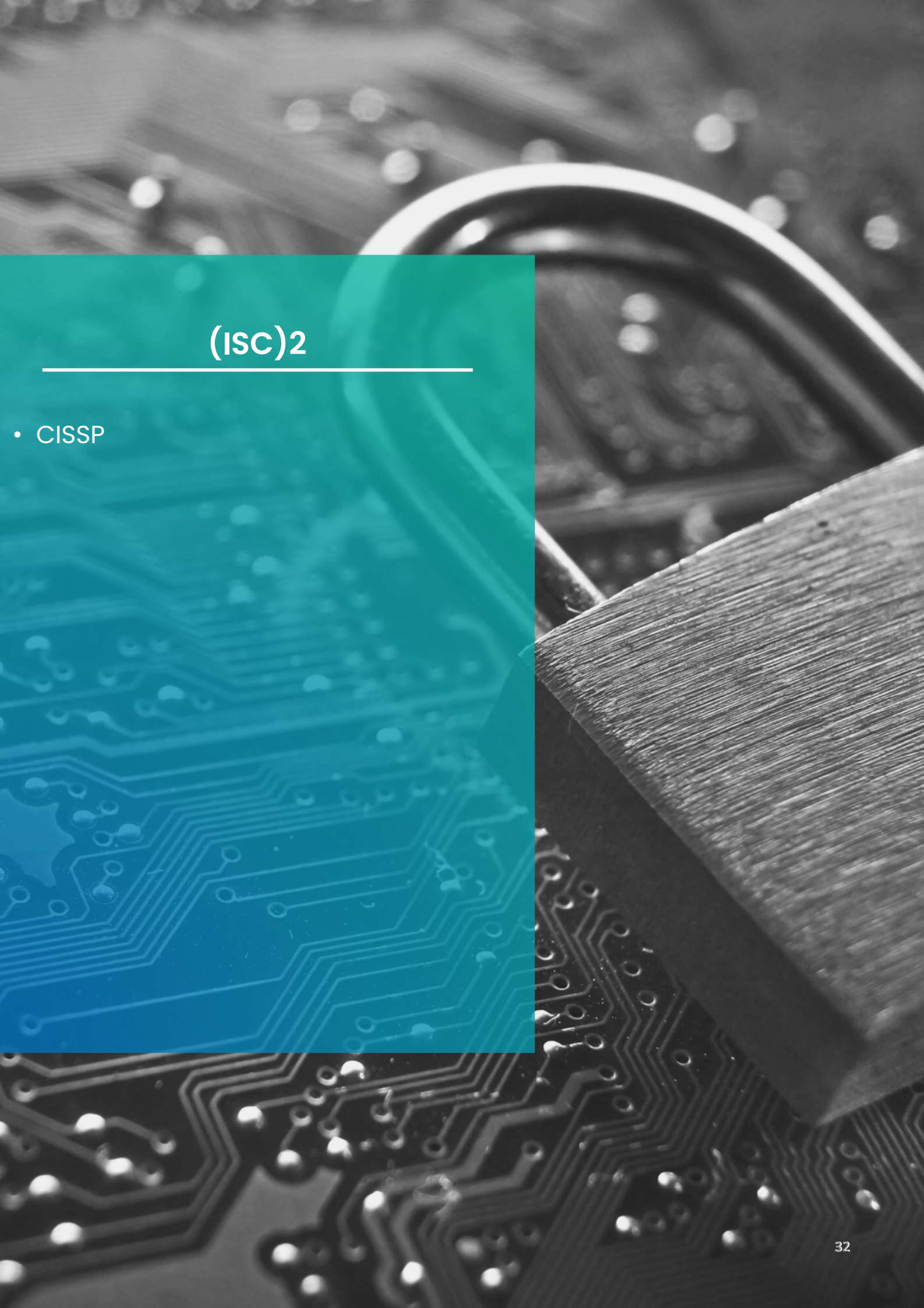
Questionnaires de satisfaction des participants

CR suite aux formations

INFORMATIONS GÉNÉRALES

Fourniture par le client de :

- 1 salle de formation 12 places min. avec vidéo projecteur
- 1 PC par personne avec 8 Go de RAM min capable de faire tourner une VM
- 1 accès Internet sur les postes



(ISC)2

- CISSP

Niveau : Expert

Durée : 5 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

RÉSUMÉ

CISSP (Certified Information Systems Security Professional) est l'une des certifications les plus prestigieuses dans le monde de la sécurité de l'information. Celle-ci atteste de vos connaissances et expérience en sécurité de l'information, en s'appuyant sur le Common Body of Knowledge (CBK), composé de 8 domaines.
La formation est dense et s'adresse aux personnes disposant déjà d'une expérience en sécurité de l'information.
L'(ISC)² améliore constamment le contenu grâce à l'engagement des experts de l'industrie, assurant que le matériel et les questions d'examen demeurent pertinents malgré les turbulences et changements courants dans le domaine de la sécurité. En définissant les huit domaines du CBK, un standard de l'industrie a été mis au point et la formation CISSP les exploite tous. Les compétences et connaissances que vous obtiendrez en suivant ce cours vous permettront de bien comprendre ces huit domaines. Elle établira crédibilité et succès pour chaque professionnel dans le domaine de la sécurité de l'information.

POUR QUI

- Professionnel de la sécurité de l'information disposant d'une expérience d'au moins 5 ans dans ce domaine.
- Si vous disposez d'une expérience de moins de 5 ans, vous pouvez toujours passer l'examen et obtenir le statut de Provisional.

OBJECTIFS PÉDAGOGIQUES

1. Gestion de la sécurité et des risques
2. Sécurité des actifs
3. Architecture de sécurité et ingénierie
4. Sécurité des communications et des réseaux
5. Évaluation et tests de la sécurité
6. Sécurité Opérationnelle
7. Sécurité des développements logiciels

CERTIFICATION

Ce cours prépare à la certification Certified Information Systems Security Professional (CISSP). Les stagiaires pourront s'inscrire individuellement. Nous recommandons aux stagiaires de prendre le temps de pratiquer des séries examens blancs avant de passer la certification, nous fournirons des listes de questions préparatoires.

Types de questions : Choix multiples et questions avancées innovantes
Compétences mesurées :

- Gestion de la sécurité et des risques 15%
- Sécurité des biens 10%
- Architecture de sécurité et ingénierie 13%
- Sécurité des communications et des réseaux 13%
- Gestion des identités et des accès (IAM) 13%
- Évaluation et tests de la sécurité 12%
- Sécurité Opérationnelle 13%
- Sécurité des développements logiciels 11%

Durée : 3 ou 6 heures

Nombre de questions : 150 à 250

Note de passage : 700/1000

Langue : Anglais

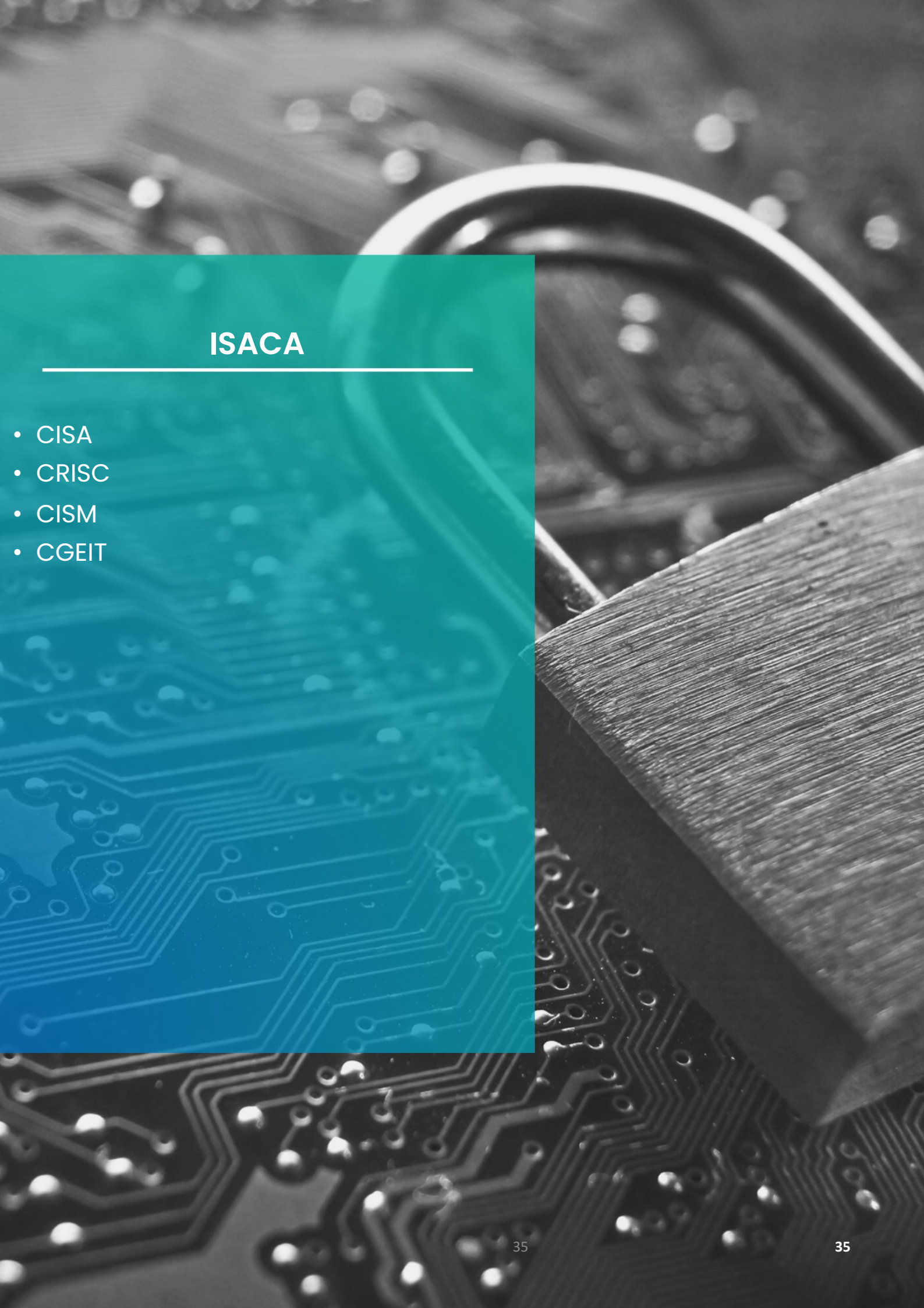
Prérequis: Il est recommandé que les participants détiennent une ou plusieurs certifications en sécurité de l'information (ISO 27001, CISM, etc.), et/ou des certifications techniques (Cisco, AWS, etc.).

MATERIEL

- Un manuel de cours
- Les livres officiels de l'ISC2, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés et accrédités par l'(ISC)^2.



ISACA

- CISA
- CRISC
- CISM
- CGEIT

35

CISA (ISACA) : PRÉPARATION À LA CERTIFICATION 1/2

Niveau : Expert

Durée : 5 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

RÉSUMÉ

CISA (Certified Information Systems Auditor) est reconnue comme l'une des certifications les plus prestigieuses en audit, contrôle, surveillance et évaluation des technologies de l'information et les systèmes d'information d'une organisation. La certification CISA est classée parmi les certifications les plus recherchées et les plus rémunératrices.
Lorsque vous aspirez à des postes de direction dans le domaine de la gestion d'un système d'information ou de l'audit, que vous veniez du monde de la technique ou du fonctionnel, la certification CISA vous apporte la visibilité et les perspectives dont vous avez besoin pour l'évolution de votre carrière.

POUR QUI

- Experts de l'audit de maturité, interne, de certification, de sous-traitants et de partenaires
- Experts de la gestion des systèmes d'information
- Tous les professionnels qui évaluent, conçoivent, déploient, pilotent et optimisent un système d'information
- DSI, RSI, RSSI, consultants stratégiques, tactiques, fonctionnels et organisationnels, techniques
- Auditeurs IT / IS, les professionnels du contrôle, de l'assurance et de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Acquérir les connaissances nécessaires à la réussite de l'examen CISA
2. Maîtriser les concepts de base de l'audit des systèmes d'information ;
3. Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information, liés à la conception et à la gestion de ces derniers ;
4. Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en audit des systèmes d'information
5. Rafraîchir ses connaissances et les concepts de base de l'audit
6. Obtenir des heures de formation continue professionnelle

CERTIFICATION

L'examen CISA dure 4 heures (240 minutes), et consiste à répondre à 150 questions à choix multiples.

Le contenu de l'examen est mis à jour régulièrement pour s'adapter aux changements produits dans la technologie et dans la pratique. Actuellement, l'examen comprend 5 sujets d'étude appelés « domaine de connaissance ».

Le pourcentage indiqué à côté de chaque domaine de connaissance correspond au pourcentage des questions qui apparaît sur ce domaine dans l'examen.

- **Domaine 1 :** processus d'audit du système d'informations (21 %)
- **Domaine 2 :** gouvernance et gestion informatique (17 %)
- **Domaine 3 :** acquisition, développement, mise en œuvre des systèmes d'informations (12 %)
- **Domaine 4 :** exploitation des systèmes d'informations et résilience des entreprises (23 %)
- **Domaine 5 :** protection des actifs informationnels (27 %)

Durée : 4 heures

Nombre de questions : 150

Note de passage : 700/1000

Langue : Anglais, français

Prérequis: Il est recommandé que les participants disposent de 5 ans d'expérience professionnelle, et détiennent une ou plusieurs certifications en audit et en gestion des systèmes d'information ou de projets.

MATERIEL

- Un manuel de cours
- Les livres officiels de l'ISACA, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés par l'ISACA.

Niveau : Expert

Durée : 3 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

RÉSUMÉ

La certification **CRISC (Certified in Risk and Information Systems Control)** de l'ISACA témoigne d'une expertise dans la gestion des risques associés aux systèmes d'information des entreprises, ainsi que dans la mise en œuvre et du maintien des contrôles des systèmes d'information.
La certification CRISC a été conçue pour valoriser les professionnels de l'informatique qui ont acquis une réelle expérience en matière d'identification, de qualification et d'évaluation des risques, d'élaboration de politique de défense, ainsi que de la prise en compte des risques dans la définition, la mise en œuvre, le suivi et la maintenance des contrôles informatiques.
La certification CRISC™ n'est pas qu'une qualification personnelle en matière de maîtrise des risques liés aux systèmes d'information. Elle aide les entreprises qui emploient les personnes certifiées à atteindre leurs objectifs « métiers » en concevant, mettant en œuvre et pilotant une politique efficace de contrôle des risques informatiques.
CRISC vous apporte la visibilité et les perspectives dont vous avez besoin pour l'évolution de votre carrière.

POUR QUI

- Experts de la gestion des risques en sécurité de l'information et de l'audit
- Tous les professionnels qui évaluent, conçoivent, déploient, supervisent et optimisent la gestion des risques de l'information avec les mesures de sécurité associées
- DSI, RSI, RSSI
- Auditeurs IT / IS, les professionnels du contrôle, de l'assurance et de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Acquérir les connaissances nécessaires à la réussite de l'examen CRISC
2. Maîtriser les concepts de la gestion de la sécurité de l'information
3. Évaluer, concevoir, déployer, superviser et améliorer tout système de gestion de la sécurité de l'information, aux plans organisationnels et techniques
4. Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information et matière de gestion de la sécurité
5. Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en gestion de la sécurité de l'information et en audit sur cette thématique

PROGRAMME & CERTIFICATION

Introduction au Certified in Risk and Information Systems Control
Domaine 1 : identification des risques informatiques
Domaine 2 : évaluation des risques informatiques
Domaine 3 : réponse et atténuation des risques
Domaine 4 : surveillance et déclaration des contrôles et des risques
Préparation à l'examen

L'examen PECB Certified Human Resources Security Foundation dure une heure. Il couvre les domaines suivants :
Domaine 1 : identification des risques informatiques (27 %)
Domaine 2 : évaluation des risques informatiques (28 %)
Domaine 3 : réponse et atténuation des risques (23 %)
Domaine 4 : surveillance et déclaration des contrôles et des risques (22 %)

Durée de l'examen: 1 heure

Type : QCM

Note de passage : 70%

Langue : Anglais, français

Prérequis: Il est recommandé que les candidats disposent d'au moins trois (3) ans d'expérience dans la gestion des risques IT et du contrôle IS. Des certifications professionnelles en gestion de la sécurité et des risques, en audit, en gestion de projet et de de services sont les bienvenues.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Un manuel de cours
- Les livres officiels de l'ISACA, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés par l'ISACA.

CISM (ISACA) : PRÉPARATION À LA CERTIFICATION 1/2

Niveau : Expert

Durée : 3 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

RÉSUMÉ

La certification ***Certified Information Security Manager® (CISM®)*** d'ISACA est conçue pour ceux qui gèrent, conçoivent, supervisent et évaluent les fonctions de la sécurité des informations d'une entreprise. Celle-ci témoigne d'une expertise dans la gouvernance de la sécurité de l'information, le développement et la gestion de programmes, la gestion des incidents et la gestion des risques.

Que vous soyez un professionnel de l'informatique ou que vous aspirez à des postes de direction dans le domaine de la sécurité et du contrôle des technologies de l'information, la certification ***CISM*** peut vous apporter la visibilité et les perspectives dont vous avez besoin.

POUR QUI

- Experts de la sécurité de l'information et de l'audit
- Tous les professionnels qui évaluent, conçoivent, déploient, supervisent et optimisent la sécurité de l'information avec les mesures de sécurité associées
- DSI, RSI, RSSI, Chief Digital Officier
- Consultants Auditeurs IT / IS, tous professionnels du contrôle, de l'assurance, de la gestion des risques et de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Acquérir les connaissances nécessaires à la réussite de l'examen CISM
2. Maîtriser les concepts de la gestion de la sécurité de l'information
3. Évaluer, concevoir, déployer, superviser et améliorer tout système de gestion de la sécurité de l'information, aux plans organisationnels et techniques
4. Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information et matière de gestion de la sécurité
5. Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en gestion de la sécurité de l'information et en audit sur cette thématique
6. Préparer l'examen CISM

CERTIFICATION

L'examen CISM dure 4 heures (240 minutes), et consiste à répondre à 150 questions à choix multiples.
Le contenu de l'examen est mis à jour régulièrement pour s'adapter aux changements produits dans la technologie et dans la pratique. Actuellement, l'examen comprend 4 sujets d'étude appelés « domaine de connaissance ».

Le pourcentage indiqué à côté de chaque domaine de connaissance correspond au pourcentage des questions qui apparaît sur ce domaine dans l'examen.

- **Domaine 1 :** gouvernance de la sécurité de l'information (24 %)
- **Domaine 2 :** gestion des risques liés à l'information (30 %)
- **Domaine 3 :** développement et gestion d'un programme de sécurité de l'information (27 %)
- **Domaine 4 :** gestion des incidents liés à la sécurité de l'information (19 %)

Durée : 4 heures

Nombre de questions : 150

Note de passage : 700/1000

Langue : Anglais, français

Prérequis: Il est recommandé que les participants disposent de 5 ans d'expérience dans un rôle de conseiller ou de superviseur dans le soutien à la gouvernance de la contribution informatique à une entreprise.
Des certifications professionnelles en gestion de la sécurité et des risques, en audit, en gestion de projet et de de services sont les bienvenues.

MATERIEL

- Un manuel de cours
- Les livres officiels de l'ISACA, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés par l'ISACA.

CGEIT (ISACA) : PRÉPARATION À LA CERTIFICATION 1/2

Niveau : Expert

Durée : 3 jours, examen à passer à la suite de la formation

Certification : inscription individuelle au passage de l'examen

RÉSUMÉ

La certification ***CGEIT (Certified in the Governance of Enterprise IT)*** de l'Isaca est une des plus prestigieuses dans le domaine de la gouvernance des technologies de l'information des entreprises. Il s'agit de la seule certification de gouvernance en informatique qui donne l'état d'esprit pour évaluer, concevoir, mettre en œuvre et gérer des systèmes de gouvernance informatique d'entreprise alignés sur les objectifs d'affaires globaux. Elle permet d'obtenir notamment auprès de la direction générale et de l'exécutif, une vision claire et précise, de la maturité, de la stratégie et de la cohérence du système d'information par rapport aux enjeux du métier.

Que vous soyez un professionnel de l'informatique ou que vous aspirez à des postes de direction dans le domaine de la gouvernance et de la stratégie informatique, la certification ***CGEIT*** peut vous apporter la visibilité et les perspectives dont vous avez besoin.

POUR QUI

- Experts de la gouvernance et de la stratégie informatique
- Tous les professionnels en matière d'alignement stratégique entre l'IT et le business, qui évaluent, conçoivent, déploient, supervisent et optimisent des systèmes d'information
- DSI, RSI, RSSI, Chief Digital Officier
- Consultants Auditeurs IT / IS, tous professionnels du contrôle, de l'assurance, de la gestion des risques et de la sécurité de l'information

OBJECTIFS PÉDAGOGIQUES

1. Acquérir les connaissances nécessaires à la réussite de l'examen CGEIT
2. Maîtriser les concepts de la gouvernance et de la stratégie informatique
3. Évaluer, concevoir, déployer, superviser et améliorer tout système d'information, aux plans organisationnels et techniques
4. Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information
5. Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en gouvernance et stratégie informatique
6. Préparer l'examen CGEIT

CERTIFICATION

L'examen CGEIT dure 4 heures (240 minutes), et consiste à répondre à 150 questions à choix multiples.
Le contenu de l'examen est mis à jour régulièrement pour s'adapter aux changements produits dans la technologie et dans la pratique. Actuellement, l'examen comprend 4 sujets d'étude appelés « domaine de connaissance ».

Le pourcentage indiqué à côté de chaque domaine de connaissance correspond au pourcentage des questions qui apparaît sur ce domaine dans l'examen.

- Domaine 1 : gouvernance informatique de l'entreprise (40 %)
- Domaine 2 : ressources informatiques (15 %)
- Domaine 3 : réalisation des avantages (26 %)
- Domaine 4 : optimisation des risques (19 %)

Durée : 4 heures

Nombre de questions : 150

Note de passage : 700/1000

Langue : Anglais, français

Prérequis: Il est recommandé que les participants disposent de 5 ans d'expérience dans un rôle de conseiller ou de superviseur dans le soutien à la gouvernance de la contribution informatique à une entreprise.
Des certifications professionnelles en gestion de la sécurité et des risques, en audit, en gestion de projet et de de services sont les bienvenues.

MATERIEL

- Un manuel de cours
- Les livres officiels de l'ISACA, ainsi que des recueils de questions de préparation à l'examen
- Un examen blanc de 150 questions

INFORMATIONS GÉNÉRALES

- Les frais de certification ne sont pas inclus dans le prix
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés par l'ISACA.

CONTINUITÉ, RÉSILIENCE, REPRISE

- ISO 22301 : Plan de continuité d'activité
- Disaster Recovery

ISO 22301 Lead Implementer – Continuité d'activité 1/2

Niveau : Expert

Durée : 5 jours

Certification : Oui

Formation éligible FNE, moncompteformation.gouv.fr : code FNE 236374

RÉSUMÉ

La formation ***ISO 22301 Lead Implementer*** permet d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la continuité d'activité et à développer vos aptitudes à fournir un cadre qui permet à l'organisation de continuer ses activités durant les crises.

POUR QUI

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

OBJECTIFS PÉDAGOGIQUES

1. Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
2. Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA
3. Savoir interpréter les exigences de la norme ISO 22301 dans un contexte spécifique de l'organisation
4. Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMCA
5. Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la continuité d'activité

PROGRAMME & CERTIFICATION

Jour 1 : Introduction à la norme ISO 22301 et initialisation d'un SMCA
Jour 2 : Planification de la mise en œuvre d'un SMCA
Jour 3 : Mise en œuvre d'un SMCA
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :

- **Domaine 1 :** Principes et concepts fondamentaux du Système de management de la continuité d'activité
- **Domaine 2 :** Système de management de la continuité d'activité
- **Domaine 3 :** Planification de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
- **Domaine 4 :** Mise en œuvre d'un SMCA conforme à la norme ISO 22301
- **Domaine 5 :** Évaluation de la performance, surveillance et mesure d'un SMCA conforme à la norme ISO 22301
- **Domaine 6 :** Amélioration continue d'un SMCA conforme à la norme ISO 22301
- **Domaine 7 :** Préparation de l'audit de certification d'un SMCA

Durée : 3 heures

Etude de cas

Note de passage : 70%

Langue : Anglais, français

Prérequis: Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de mise en œuvre.

MATERIEL & INGENIERIE PEDAGOGIQUE

En plus du matériel de cours de PECB, Formind Academy fournit un livret qui comprend une étude de cas adaptée au marché français. Cette étude de cas s'appuie sur l'expérience terrain de nos formateurs et consultants.

Un manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques est fourni aux participants

Les cours sont illustrés par des questions pratiques et des exemples

Les exercices pratiques comprennent des exemples et des discussions

Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

ISO 22301 Lead Auditor – Continuité d'activité 1/2

Niveau : Expert

Durée : 5 jours

Certification : Oui

Formation éligible FNE, moncompteformation.gouv.fr : code FNE 235906

RÉSUMÉ

La formation ***ISO 22301 Lead Auditor*** permet d'acquérir l'expertise nécessaire pour réaliser des audits de Système de management de la continuité d'activité (SMCA) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues. Durant cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes, en conformité avec la norme ISO 19011 et le processus de certification d'ISO/CEI 17021-1.
Grâce aux exercices pratiques, vous serez en mesure de maîtriser les techniques d'audit et disposerez des compétences requises pour gérer un programme d'audit, une équipe d'audit, la communication avec les clients et la résolution de conflits.

POUR QUI

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la continuité d'activité
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la continuité d'activité
- Experts techniques désirant préparer un audit du Système de management de la continuité d'activité
- Conseillers spécialisés en management de la continuité d'activité

OBJECTIFS PÉDAGOGIQUES

1. Comprendre le fonctionnement d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301
2. Expliquer la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
3. Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
4. Savoir diriger un audit et une équipe d'audit
5. Savoir interpréter les exigences d'ISO 22301 dans le contexte d'un audit du SMCA
6. Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

ISO 22301 Lead Auditor – Continuité d'activité 2/2

PROGRAMME & CERTIFICATION

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

L'examen couvre les domaines de compétences suivants :

- **Domaine 1 :** Principes et concepts fondamentaux du Système de management de la continuité d'activité
- **Domaine 2 :** Système de management de la continuité d'activité (SMCA)
- **Domaine 3 :** Principes et concepts fondamentaux de l'audit
- **Domaine 4 :** Préparation d'un audit ISO 22301
- **Domaine 5 :** Réalisation d'un audit ISO 22301
- **Domaine 6 :** Clôturer un audit ISO 22301
- **Domaine 7 :** Gérer un programme d'audit ISO 22301

Durée : 3 heures	Etude de cas	Note de passage : 70%	Langue : Anglais, français

Prérequis: Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de mise en œuvre.

MATERIEL & INGENIERIE PEDAGOGIQUE

En plus du matériel de cours de PECB, Formind Academy fournit un livret qui comprend une étude de cas adaptée au marché français. Cette étude de cas s'appuie sur l'expérience terrain de nos formateurs et consultants.

Un manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques est fourni aux participants

Les cours sont illustrés par des questions pratiques et des exemples

Les exercices pratiques comprennent des exemples et des discussions

Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

Lead Disaster Recovery Manager 1/2

Niveau : Expert

Durée : 5 jours, examen inclus

Certification :PECB Certified Lead Disaster Recovery Manager

RÉSUMÉ

La formation ***Lead Disaster Recovery Manager*** vous permettra d'acquérir l'expertise nécessaire pour soutenir une organisation dans la mise en œuvre, le maintien et la gestion d'un plan en cours de reprise d'activité après sinistre. Durant cette formation, vous obtiendrez également une connaissance approfondie des meilleures pratiques relatives au processus de reprise d'activité après sinistre et des services de reprise après sinistre des TIC dans le cadre de la gestion de la continuité des activités.

Après avoir maîtrisé l'ensemble des concepts nécessaires aux processus de la reprise d'activité après sinistre, vous pouvez vous présenter à l'examen et postuler au titre de ***PECB Certified Lead Disaster Recovery Manager***. En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger les équipes chargées de la reprise d'activité après sinistre durant la mise en œuvre des stratégies de reprise d'activité après sinistre en conformité avec les meilleures pratiques.

POUR QUI

- Professionnels ou consultants en reprise d'activité après sinistre souhaitant acquérir une connaissance approfondie des concepts et des processus nécessaires liés aux stratégies de reprise d'activité
- Gestionnaires chargés d'établir un plan de reprise d'activité après sinistre dans une organisation
- Personnes responsables de la conformité aux exigences relatives à la reprise d'activité après sinistre dans une organisation
- Membres d'une équipe chargée de la reprise d'activité après sinistre

OBJECTIFS PÉDAGOGIQUES

1. Connaître la corrélation entre la reprise d'activité après sinistre, la gestion de la continuité des activités, la sécurité de l'information et d'autres domaines et cadres informatiques
2. Maîtriser les concepts, approches, méthodes et techniques nécessaires pour la mise en œuvre et la gestion efficace des services de reprise d'activité après sinistre
3. Savoir interpréter les stratégies de reprise d'activité des TIC dans le contexte spécifique d'une organisation
4. Apprendre à soutenir un organisme afin de planifier, mettre en œuvre, gérer, surveiller et entretenir efficacement les services de reprise d'activités après sinistre en conformité avec les meilleures pratiques
5. Acquérir l'expertise nécessaire pour conseiller une organisation en matière de reprise d'activité après sinistre

Lead Disaster Recovery Manager 2/2

PROGRAMME & CERTIFICATION

Jour 1 : Introduction à la reprise d'activité après sinistre et lancement d'un plan de reprise d'activité après sinistre
Jour 2 : Stratégies d'atténuation des risques et planification de la reprise d'activité après sinistre
Jour 3 : Services de reprise d'activité après sinistre, sites de récupération, installations, réponse et activation
Jour 4 : Test, suivi, mesure et amélioration continue du plan de reprise d'activité après sinistre
Jour 5 : Examen de certification

L'examen couvre les domaines de compétences suivants :

- **Domaine 1 :** Principes et concepts fondamentaux du plan de reprise d'activité après sinistre
- **Domaine 2 :** Développement du plan de reprise d'activité après sinistre
- **Domaine 3** : Sous-sections de support de reprise après sinistre
- **Domaine 4 :** Sites de récupération, installations de récupération et capacité des services externalisés
- **Domaine 5 :** Test et tenue à jour d'un plan de reprise après sinistre
- **Domaine 6** : Amélioration continue d'un plan de reprise d'activité après sinistre

Durée : 3 heures

Type : étude de cas

Note de passage : 70%

Langue : Anglais, français

Prérequis: Une compréhension fondamentale des services de reprise d'activité après sinistre et une connaissance approfondie des principes, des concepts et des stratégies de gestion.

MATERIEL & INGENIERIE PEDAGOGIQUE

- Livret comprenant étude de cas et ensemble de questions de préparation à l'examen
- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur la théorie et sur les meilleures pratiques utilisées dans l'la mise en œuvre et la gestion d'un plan de reprise d'activité après sinistre
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Exercices pratiques basés sur une étude de cas incluant des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

DÉVELOPPEMENT INVESTIGATION NUMERIQUE

- Développements sécurisés
- Investigation sur incident de sécurité

Développements sécurisés 1/2

Niveau : Expert

Durée : 2 jours

Prérequis: Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité. Connaissance des langages de programmations C, C++, Java, etc

RÉSUMÉ

Le logiciel est partout dans les dispositifs que nous utilisons au quotidien : ordinateurs, mobiles, objets connectés, voitures, … Le développement sécurisé consiste à protéger d'une part les logiciels et les environnements sur lesquels ils s'exécutent, mais aussi d'intégrer dans les pratiques de développement la sécurité comme une responsabilité de chacun des contributeurs.
Dans cette formation, nous présentons et expliquons les principales sources de vulnérabilités présentes dans les logiciels codés en C et C++ (mais ils sont applicables à l'ensembles de langages de programmation). Nous nous appuyons sur les recommandations d'organismes référents tels que le SEI, le CERT, le MITRE, le NIST, l'ANSSI et surtout l'OWASP. L'objectif est de sensibiliser aux principales vulnérabilités d'applications web et de former les participants à la défense en profondeur par une approche offensive que l'on appelle Bug Bounty, d'apprendre à corriger ces failles de manière ludique.
Par défaut, nous appuyons ce cours sur les langages C et le C++, qui sont largement utilisés pour développer les briques logicielles essentielles de ces dispositifs (OS, firmware, drivers, applications, …). Mais d'autres langages sont disponibles comme le PHP ou l'Angular et Java spring.

POUR QUI

- Toute personne impliquée dans le développement, la mise en production et le suivi des logiciels
- Développeurs, chefs de projet, auditeurs.
- Environnements Linux, Windows, systèmes embarqués

OBJECTIFS PÉDAGOGIQUES

1. Comprendre le développement logiciel en tenant compte dès sa spécification
2. Comprendre l'intérêt des concepts de Secure Coding et Secure by Design
3. Connaitre et appliquer des techniques de conception et de développement en vue de protéger les logiciels, les systèmes hôtes et leur environnement
4. Savoir identifier et détecter des failles de sécurité et éviter leur(s) conséquence(s)
5. Mettre en place des pratiques d'audit et de tests en vue d'identifier au plus tôt des vulnérabilités de code
6. Savoir réduire les surfaces d'attaques d'un système
7. Connaitre les recommandations SEI CERT, OWASP quant aux bonnes pratiques de développent C/C++
8. Savoir consulter le classement CVE des vulnérabilités en lien avec les développements C/C++

PROGRAMME & CERTIFICATION

La formation se déroule sur deux jours en présentiel avec un formateur. Un quart du temps est dédié à une approche théorique de la sécurité applicative. Le reste es dédié à la pratique sous forme de bug Bounty.

Contenu de la formation et approche :

- Présentation théorique des référentiels de vulnérabilité
- Présentation des principales vulnérabilités du TOP10 OWASP
- Apprendre par le jeu et la mise en pratique permet de faire passer des messages rapidement et de les intégrer dans la durée.
- Apprendre à entrer dans la peau de hackers
- Apprendre à identifier les vulnérabilités et à les corriger.
- Par équipes de deux : compétition de type CTF.
- Objectif de découvrir les vulnérabilités et identifier la bonne correction à appliquer Si c'est correct : des points sont gagnés !
- Analyse à partir du code source de l'application

Déroulement de la formation :

- journée 1
  - Introduction (3h), Tour de table, Objectifs
  - Principales vulnérabilités
  - Mise en place du jeu (30min), Règles du jeu
  - Démarrage des environnements
  - Présentation des outils
  - Jeu bug bounty (4h30)
  - Compétition par équipe
  - 30 vulnérabilités à trouver
  - Débriefings

- journée 2
  - Jeu bug bounty (5h)
  - Compétition par équipe
  - 30 vulnérabilités à trouver
  - Débriefings réguliers
  - Fin du jeu et correction (2h30)
  - Démonstration des vulnérabilités du jeu
  - Questions/réponses
  - Conclusion (30min)

MATERIEL & INGENIERIE PEDAGOGIQUE

Le cours s'appuie sur les standards actuels. Chaque thématique est illustrée d'exemples expliqués réels et récents.
Dans le but de comprendre les concepts et de s'exercer efficacement, les parties pratiques s'appuient sur la réalisation d'exploitations de vulnérabilités, leur analyse, et sur l'audit de codes.
Ces exercices pratiques se feront à partir du l'ordinateur de l'apprenant disposant d'un accès internet et d'un logiciel de virtualisation.

INFORMATIONS GÉNÉRALES

- Fourniture des supports de formation et de fiches pratiques.
- Une attestation de participation sera délivrée.
- Mise à disposition d'une machine virtuelle vulnérable.
- Nous garantissons la qualité de formations.

Investigation numérique - réseau et Windows 1/2

Niveau : Expert

Durée : 5 jours

Certification : Non

RÉSUMÉ

Cette formation intensive en investigation numérique a pour objectif de former les participants à réagir efficacement face à un incident de sécurité informatique, en se concentrant sur un cas typique d'attaque par ransomware. Les participants apprendront les compétences essentielles nécessaires pour identifier, contenir, analyser et remédier à une telle attaque.
La formation se déroule sous forme de sessions théoriques interactives, de démonstrations pratiques et d'exercices en laboratoire. Les participants seront confrontés à un scénario réaliste, où ils devront travailler en équipe pour enquêter, analyser et partager les résultats d'investigation sur une incident de ransomware.

Les participants seront prêts à réagir de manière proactive et efficace face à des cyber attaques et à contribuer à la protection des systèmes d'information de leur organisation.
Cette formation est un moyen concret pour les participants d'acquérir une expérience pratique et de se préparer à faire face aux menaces croissantes dans l'environnement numérique actuel.

POUR QUI

- Administrateur systèmes et réseaux
- Responsable d'exploitation
- Responsable de la sécurité des systèmes d'information
- Analyste SOC / CERT

OBJECTIFS PÉDAGOGIQUES

1. Apprendre à réagir efficacement face à des incidents de sécurité informatique.
2. Apprendre à collecter, préserver et documenter des preuves numériques, en utilisant des outils et des techniques appropriés.
3. Apprendre à rédiger des rapports d'enquête complets.
4. Développer des compétences avancées en matière d'analyse de données numériques et en identification de comportements suspects.
5. Acquérir une connaissance approfondie des concepts tels que le modèle MITRE ATT&CK, la Kill Chain, les Indicateurs de Compromission et la Pyramid of Pain.

PROGRAMME & CERTIFICATION

Jour 1 : La réponse à incident et ses standards
Jour 2 : L'acquisition de preuves et les techniques
Jour 3 : Les artefacts et les techniques d'analyse
Jour 4 : Analyse mémoire et de fichier malveillant
Jour 5 : Mise en pratique et formalisation des analyses

Connaissance et prérequis :

- Réseaux, TCP/IP, connaissances sur les protocoles
- Système Windows & Active Directory
- Linux et logiciels de la distribution Kali
- Coding/programmation : Bases requises (python, powershell, C, php, word/excel)

MATERIEL & INGENIERIE PEDAGOGIQUE

- Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques
- Formation basée sur un cas d'incident mêlant la théorie et la pratique
- Exercices pratiques basés sur un incident de type ransomware
- Les tests pratiques sont similaires à l'examen de certification

INFORMATIONS GÉNÉRALES

- Une attestation de participation sera délivrée.
- Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité,
- Cette formation se veut très axées sur la pratique

PROTECTION DES DONNÉES PERSONNELLES

- RGPD
- Certification des compétences du DPO (CNIL)

RGPD – Introduction

Niveau : Sensibilisation

Durée : 1 jour

Certification : non

RÉSUMÉ

La formation *Introduction au RGPD* permet d'appréhender les concepts de base et les exigences du Règlement général de la protection des données (RGPD). En participant au cours d'introduction au RGPD, vous allez comprendre l'importance du RGPD et les avantages que les entreprises, la société et les gouvernements peuvent en tirer.

POUR QUI

- Aux personnes intéressées par les principes fondamentaux de protection de la vie privée
- Aux personnes souhaitant acquérir des connaissances sur les principales exigences du règlement général sur la protection des données (RGPD)

OBJECTIFS PÉDAGOGIQUES

Comprendre les principes fondamentaux de protection de la vie privée et l'histoire de la protection des données personnelles en Europe
Comprendre les concepts de base et les exigences du règlement général sur la protection des données (RGPD)

PROGRAMME & CERTIFICATION

Jour 1 : Introduction au Règlement Général sur la Protection des Données (RGPD)

Aucun prérequis

MATERIEL & INGENIERIE PEDAGOGIQUE

Manuel de cours contenant plus de 100 pages d'informations et d'exemples pratiques

INFORMATIONS GÉNÉRALES

Nous garantissons la qualité de formations. Nos formateurs sont des professionnels de la cyber sécurité, certifiés Approved Trainer par PECB et/ou l'APMG.

RGPD – Certified Data Protection Officer 1/2

Niveau : Expert

Durée : 5 jours

Certification : passage de l'examen inclus

Formation éligible FNE, moncompteformation.gouv.fr : code FNE 237373

RÉSUMÉ

La formation ***Certified Data Protection Officer*** de PECB permet d'acquérir les connaissances et les compétences nécessaires, et de développer la compétence nécessaire pour remplir le rôle de délégué à la protection des données dans la mise en œuvre d'un programme de conformité au RGPD.
La protection des données devenant de plus en plus précieuse, la nécessité pour les organismes de protéger ces données ne cesse d'augmenter elle aussi. Outre la violation des droits et libertés fondamentaux des personnes, le non-respect de la réglementation en matière de protection des données peut entraîner des situations risquées susceptibles de nuire à la crédibilité, à la réputation et à la situation financière d'un organisme. C'est là que vos compétences en tant que responsable de la protection des données entrent en jeu.

POUR QUI

- Gestionnaires ou consultants souhaitant préparer et soutenir un organisme dans la planification, la mise en œuvre et le maintien d'un programme de conformité basé sur le RGPD
- DPO et personnes responsables du maintien de la conformité aux exigences du RGPD
- Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité d'activité
- Experts techniques et experts de la conformité envisageant un poste de délégué à la protection des données
- Conseillers experts en sécurité des données personnelles

OBJECTIFS PÉDAGOGIQUES

1. Comprendre les concepts du RGPD et interpréter ses exigences
2. Comprendre le contenu et la corrélation entre le Règlement général sur la protection des données et d'autres cadres réglementaires et normes applicables, telles que ISO/IEC 27701 et ISO/IEC 29134
3. Acquérir la compétence nécessaire pour remplir le rôle et les tâches quotidiennes du délégué à la protection des données au sein d'un organisme
4. Développer la capacité à informer, conseiller et surveiller la conformité au RGPD et à coopérer avec l'autorité de surveillance

RGPD – Certified Data Protection Officer 2/2

PROGRAMME & CERTIFICATION

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

L'examen *PECB Certified Data Protection Officer* répond pleinement aux exigences du Programme d'examen et de certification PECB (PEC). L'examen couvre les domaines de compétence suivants :

- Domaine 1 : Concepts de protection des données, Règlement général sur la protection des données (RGPD), et mesures de conformité
- Domaine 2 : Rôles et responsabilités des parties responsables de la conformité au RGPD
- Domaine 3 : Mesures techniques et organisationnelles pour la protection des données

Durée de l'examen: 3 heures

Type : Etude de cas

Note de passage : 70%

Langue : Anglais, français

Prérequis: Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données.

MATERIEL & INGENIERIE PEDAGOGIQUE

En plus du matériel de cours de PECB, Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants.

Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques

Les participants sont encouragés à échanger et à s'engager dans les discussions et les exercices.

Les exercices pratiques et les quiz sont semblables aux questions de l'examen de certification.

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- Le support de formation contenant plus de 200 pages d'informations et d'exemples pratiques sera distribué
- Une attestation de participation de 14 crédits DPC (Développement professionnel continu) sera délivrée.
- Nous garantissons la qualité de formations. En cas d'échec à l'examen, vous pouvez le reprendre dans les 12 mois suivants sans frais additionnels.

Certification des compétences du DPO (CNIL) 1/2

Niveau : Expert

Durée : 5 jours

Certification : passage de l'examen inclus

RÉSUMÉ

Validez vos compétences en tant que ***DPO*** avec la certification PECB selon les exigences de la CNIL
PECB est agréée par la CNIL depuis le 15 octobre 2020 (Délibération n° 2020-099) pour la certification des compétences du délégué à la protection des données en conformité avec les Délibérations n° 2018-317 et n° 2018-318 du 20 septembre 2018 de la CNIL.
Vous souhaitez démontrer que vous détenez les compétences du DPO en conformité avec les référentiels de la CNIL ? Inscrivez-vous rapidement et faites reconnaître les compétences acquises selon les référentiels de la CNIL.
PECB à travers son réseau de revendeurs des formations PECB agréés, vous propose une formation pour vous préparer à la certification des compétences du délégué à la protection des données conformément aux référentiels de la CNIL. Cette formation n'est pas exclusive et d'autres formations suivies par les candidats seront aussi recevables, sous réserve qu'elles portent sur la protection des données personnelles et qu'elles soient d'au moins 35 heures, conformément au référentiel de certification de la CNIL.

POUR QUI

Prérequis pour la certification initiale - Durée de validité de la certification : 3 ans
Justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles ; ou
Justifier d'une expérience professionnelle d'au moins 2 ans ainsi que d'une formation d'au moins 35 heures en matière de protection des données personnelles reçue par un organisme de formation.

Renouvellement de la certification
Le renouvellement de la certification est possible avant la date d'échéance du certificat à condition que la personne certifiée :
Réussisse une nouvelle épreuve écrite répondant aux exigences de la catégorie 2 du présent référentiel ; et
Démontrer qu'elle dispose d'une expérience professionnelle d'au moins un an, acquise dans le courant des trois dernières années, dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données ou de la sécurité de l'information, attestée par un tiers (employeur ou client).

OBJECTIFS PÉDAGOGIQUES

1. Bénéficier de la reconnaissance internationale de PECB et obtenir un certificat conforme aux exigences de la CNIL
2. Bénéficier d'un processus de certification rapide
3. Prouver que vous possédez les compétences de DPO
4. Bénéficier d'un avantage concurrentiel
5. Examen QCM élaboré par des experts selon les exigences de la CNIL

PROGRAMME & CERTIFICATION

Jour 1 : Introduction aux principes et concepts du RGPD
Jour 2 : Désignation du DPO et analyse du programme de conformité au RGPD
Jour 3 : Responsabilités opérationnelles du DPO
Jour 4 : Suivi et amélioration continue de la conformité au RGPD
Jour 5 : Toolkit RGPD (Pratique et analyse)

L'examen *Délégué à la protection des données certifié conformément au référentiel de certification des compétences du DPO de la CNIL* comprend 100 questions à choix multiple, en français, et couvre les trois domaines suivants :

- Domaine 1 : Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
- Domaine 2 : Responsabilité
- Domaine 3 : Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

Aucun support n'est utilisé pendant l'examen. Pour chaque question, quatre réponses sont proposées dont une seule est exacte.

Durée de l'examen: 3 heures	Type : QCM	Note de passage : 75% (50% dans chaque domaine)	Langue : français

Prérequis: Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données.

MATERIEL & INGENIERIE PEDAGOGIQUE

En plus du matériel de cours de PECB, Formind Academy fournit une étude de cas, adaptée au marché français et européen, qui s'appuie sur l'expérience terrain de nos formateurs et consultants.

Manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques

Les participants sont encouragés à échanger et à s'engager dans les discussions et les exercices.

Les exercices pratiques et les quiz sont semblables aux questions de l'examen de certification.

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- Nous garantissons la qualité de formations. En cas d'échec à l'examen, vous pouvez le reprendre dans les 12 mois suivants sans frais additionnels.

FORMATIONS À LA DEMANDE

- Devops
  - Devops Fundamentals
  - DevOps Leadership
- Agile Scrum
  - Professional Scrum Master
- Togaf et l'architecture d'entreprise
  - Niveaux Foundation & Certified
- ITIL et la gestion des services
  - Itil Foundation
- Prince2 et la Gestion de projets
  - Prince2 Foundation & Practitionner
- Lean Six Sigma et l'optimisation des organisations
  - Lean IT
  - Yellow Belt
  - Green Belt
  - Black Belt

MERCI

NOUS CONTACTER

formation@formind.fr

Possibilité d'inscription en ligne :

https://www.formind.fr/formation/

formind
7 chemin de Bretagne
92130 Issy-les-Moulineaux

formind
ACADEMY