CATALOGUE FORMATIONS

ÉDITION 2024

KYRON

Your Cyber our Concern

CONSOLIDER, ACQUÉRIR

C'est avec grand plaisir que je vous laisse découvrir notre catalogue Formations qui représente le fruit d'un travail collaboratif au sein de KYRON.

Nos formations ont pour objectif de permettre à tout participant de consolider ou acquérir les connaissances nécessaires à la compréhension de la cybersécurité en environnement OT et IT. Notre équipe de spécialistes formés et certifiés, comprend les enjeux et répond concrètement aux attentes et aux besoins spécifiques des organisations.

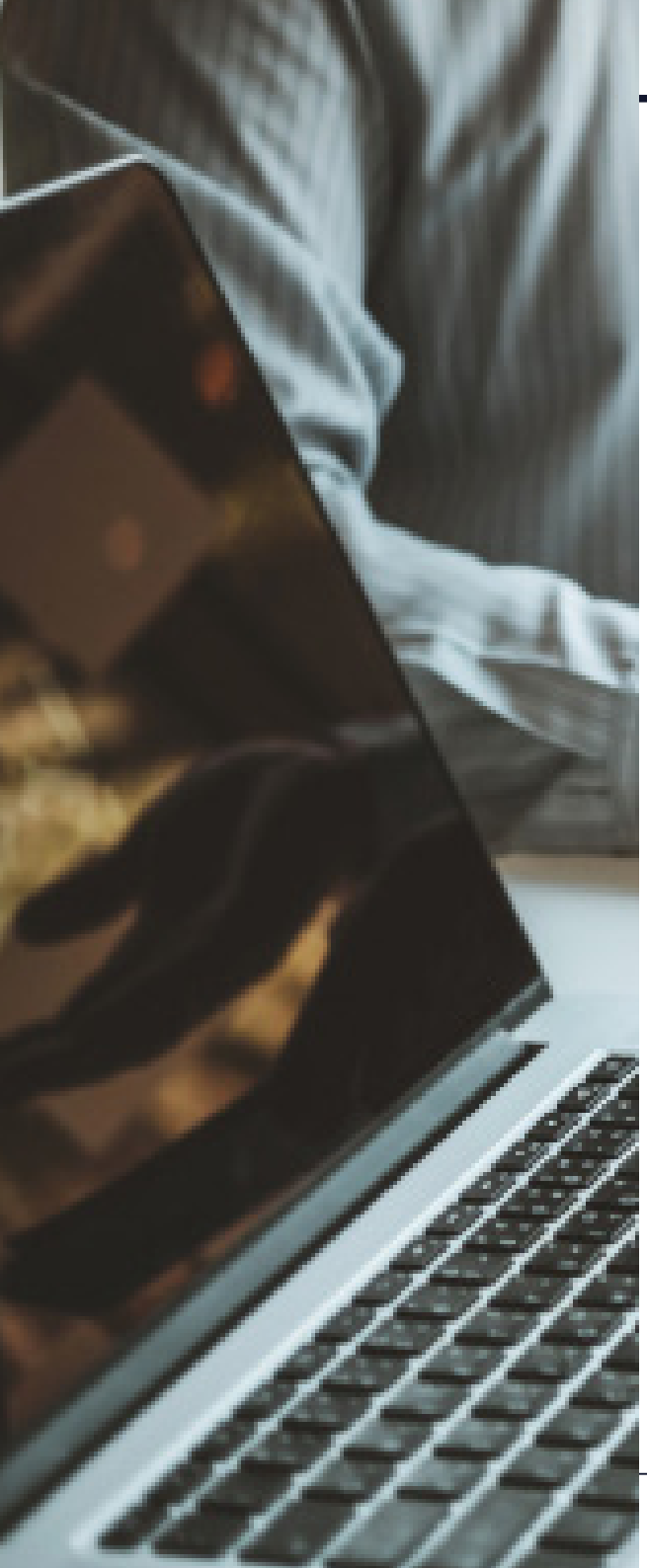
Nos formations traitent un ensemble de sujets liés à la cybersécurité OT et IT et sont conçues pour répondre aux besoins métiers des environnement industriels, des outils de productions et d'informatique de gestion. Les services de KYRON se différencient en ciblant un objectif d'expertises et de certifications associé au monde industriel, afin de disposer des doubles compétences reconnues de haut niveau. Le but étant d'aligner les équipes de sécurité OT et IT afin de répondre aux enjeux métiers de chacun.

La bonne formation au bon moment pour répondre à vos besoins.

Je vous souhaite une bonne formation avec notre équipe !

Hakim Bendib
Président

SOMMAIRE



Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité à été délivrée au titre de la catégorie d'action suivante : **Action de formation**

Pour de plus amples informations, veuillez nous contacter à l'adresse training@kyron.fr ou par téléphone au+33 (0)5 34 47 86 65

CALENDRIER DE FORMATIONS

JANVIER

LEAD CLOUD SECURITY MANAGER	**15 au 19**
ISO 27001 LEAD IMPLEMENTER	**22 au 26**

FÉVRIER

ISO 27005 RISK MANAGER	**12 au 14**
ISA/IEC 62443 IC32	**15 au 16**
LEAD ETHICAL HACKER	**19 au 23**
RISK MANAGER MÉTHODE EBIOS	**26 au 28**

MARS

LEAD SCADA SECURITY MANAGER	**04 au 08**
ISO 27001 LEAD IMPLEMENTER	**12 au 15**
ISO 27001 LEAD AUDITOR	**18 au 22**
LEAD ETHICAL HACKER	**25 au 29**

AVRIL

RISK MANAGER MÉTHODE EBIOS	**08 au 10**
ISA/IEC 62443 IC33	**17 au 19**
LEAD CLOUD SECURITY MANAGER	**22 au 26**
ISO 27001 FOUNDATION	**29 au 30**

MAI

ISO 27001 LEAD IMPLEMENTER	**06 au 10**
CMMC FOUNDATION	**28 au 29**
ISO 27001 LEAD AUDITOR	**19 au 23**
ISO 27005 RISK MANAGER	**29 au 31**

JUIN

LEAD ETHICAL HACKER	**03 au 07**
ISA/IEC 62443 IC34	**12 au 14**
ISO 27001 LEAD AUDITOR	**17 au 21**
LEAD SCADA SECURITY MANAGER	**24 au 28**

**Nous consulter pour avoir des renseignements sur les formations non listées ci-dessus.*

**Nous consulter pour avoir des renseignements sur les formations non listées ci-dessous.*

JUILLET

LEAD SCADA SECURITY MANAGER	**03 au 07**
ISO 27005 RISK MANAGER	**15 au 17**
ISO 27001 LEAD IMPLEMENTER	**22 au 26**
ISO 27001 LEAD AUDITOR	**20 au 24**

AOUT

LEAD CLOUD SECURITY MANAGER	**04 au 08**
ISO 27005 RISK MANAGER	**13 au 15**
ISO 27001 FOUNDATION	**29 au 30**

SEPTEMBRE

LEAD SCADA SECURITY MANAGER	**02 au 06**
ISA/IEC 62443 IC37	**11 au 13**
LEAD ETHICAL HACKER	**16 au 20**
RISK MANAGER MÉTHODE EBIOS	**23 au 25**
CMMC FOUNDATION	**26 au 27**

OCTOBRE

ISO 27001 LEAD IMPLEMENTER	**06 au 10**
LEAD ETHICAL HACKER	**14 au 18**
ISO 27001 LEAD AUDITOR	**21 au 25**
ISO 27005 RISK MANAGER	**28 au 30**
CMMC FOUNDATION	**31 au 01/11**

NOVEMBRE

LEAD CLOUD SECURITY MANAGER	**04 au 08**
RISK MANAGER MÉTHODE EBIOS	**13 au 15**
LEAD SCADA SECURITY MANAGER	**18 au 22**
CMMC FOUNDATION	**26 au 27**

DECEMBRE

LEAD SCADA SECURITY MANAGER	**02 au 06**
LEAD ETHICAL HACKER	**09 au 13**

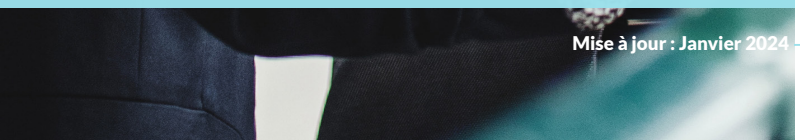
KYRON

DEVENEZ UN PROFESSIONNEL DE LA SÉCURITÉ SCADA

La formation SCADA Security Manager vous permet de développer l'expertise nécessaire pour planifier, concevoir et mettre en œuvre un programme efficace de protection des systèmes SCADA. En outre, vous serez en mesure de comprendre les menaces, les vulnérabilités et les risques courants liés aux systèmes de contrôle industriel (ICS) et les techniques utilisées pour gérer ces risques.

Cette formation met l'accent sur plusieurs aspects de la gestion de la sécurité et sur les compétences liées à la sécurité des SCADA/ICS. Le cours de formation Lead SCADA Security Manager est conçu par des experts du secteur ayant une expérience approfondie de la sécurité des systèmes SCADA et des systèmes de contrôle industriel. Contrairement à d'autres formations, cette formation se concentre spécifiquement sur les connaissances et les compétences nécessaires à un professionnel souhaitant devenir responsable de la sécurité des systèmes SCADA et des systèmes de contrôle industriels mais aussi les compétences nécessaires à un professionnel souhaitant donner des conseils ou gérer les risques liés aux environnements et systèmes SCADA. Compte tenu de la nature très visible et les impacts significatifs associés à ces environnements, une approche professionnelle holistique de la sécurité est nécessaire et c'est exactement ce que ce cours est conçu pour fournir.

En outre, pour acquérir les connaissances théoriques nécessaires à un responsable de la sécurité SCADA, une méthodologie complète pour la mise en œuvre d'un programme de sécurité SCADA est proposée. Ainsi, à la fin de ce cours, vous acquerrez des connaissances sur la façon de mettre en œuvre efficacement un programme de sécurité pour les systèmes SCADA/ICS.



Mise à jour : Janvier 2024

F-LEADSCADA

LEAD SCADA SECURITY MANAGER

FORMATION CERTIFIÉE PECB

PUBLIC

Professionnels de la sécurité souhaitant acquérir des compétences professionnelles en matière de sécurité SCADA, professionnels de l'informatique souhaitant améliorer leurs compétences et connaissances techniques, responsables informatiques et gestionnaires de risques souhaitant acquérir une connaissance plus approfondie des systèmes ICS et SCADA, développeurs de systèmes SCADA, professionnels de l'informatique SCADA, ingénieurs et opérateurs SCADA.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Une compréhension fondamentale de la sécurité SCADA. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre et expliquer l'objectif et les risques des systèmes SCADA, des systèmes de contrôle distribués et des contrôleurs logiques programmables
- Développer l'expertise nécessaire pour soutenir un programme proactif de sécurité SCADA, y compris les politiques et la gestion des vulnérabilités
- Définir et concevoir une architecture de réseau intégrant des contrôles de sécurité avancés pour SCADA
- Expliquer la relation entre les contrôles de gestion, opérationnels et techniques dans un programme de sécurité SCADA
- Améliorer la capacité à concevoir des systèmes SCADA résilients et à haute disponibilité.
- Apprendre à gérer un programme d'activités de tests de sécurité efficaces

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified Provisional SCADA Security Manager* ou *Certified SCADA Security Manager* ou *Certified Lead SCADA Security Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux de SCADA et de la sécurité SCADA
2 : Caractéristiques, menaces et vulnérabilités des systèmes de contrôle industriels (ICD)
3 : Concevoir et développer un programme de sécurité ICS basé sur le NIST SP 800-82
4 : Architecture de sécurité du réseau pour les systèmes SCADA
5 : Mise en œuvre de contrôles de sécurité pour les systèmes SCADA
6 : Développer des systèmes résilients et robustes
7 : Test de sécurité des systèmes SCADA

PROGRAMME

Jour 1 : Introduction à SCADA et ICS
Objectifs et structure du cours, principes et concepts fondamentaux de SCADA et de la sécurité SCADA, caractéristiques, menaces et vulnérabilités des systèmes de contrôle industriel (SCI)

Jour 2 : Conception d'un programme de sécurité et d'une architecture de sécurité du réseau
Programme de sécurité SCADA, évaluation des risques, architecture de sécurité du réseau pour les systèmes SCADA

Jour 3 : Mise en œuvre des contrôles de sécurité du SCI, gestion des incidents et continuité des activités
Mise en œuvre de contrôles de sécurité pour les systèmes SCADA, gestion des incidents, lien avec la continuité des activités, suivi, analyse des mesures et évaluation

Jour 4 : Tests de sécurité des systèmes SCADA
Principes de test, questions juridiques et éthiques, approches des tests de pénétration, tests de sécurité des ICS, gestion d'un test d'intrusion, documentation de l'essai, examen de la qualité, maintien d'un programme d'essais, compétence et évaluation des responsables de la sécurité SCADA

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

Ce cours offre un aperçu détaillé de la manière dont les normes ISA/IEC 62443 peuvent être utilisées pour protéger vos systèmes de contrôle critiques. Il explore également les différences procédurales et techniques entre la sécurité pour les environnements informatiques traditionnels et les solutions appropriées pour les environnements SCADA ou d'usine. Le cours explore l'évolution vers l'utilisation de normes ouvertes telles qu'Ethernet, TCP/IP et les technologies web dans les réseaux SCADA et de contrôle de processus, qui a commencé à exposer ces systèmes aux mêmes cyber-attaques qui ont fait tant de ravages dans les systèmes d'information des gouvernements et des entreprises.

Mise à jour : Janvier 2024

F-ISAFS-IC32

ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST

FORMATION CERTIFIÉE

PUBLIC

Il n'y a pas de conditions préalables requises pour suivre ce cours. Toutefois, il est fortement recommandé aux candidats d'avoir au moins un à trois ans d'expérience dans le domaine de la cybersécurité, avec une certaine expérience dans un environnement industriel.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

PRÉREQUIS

Cours ISA : TS06, TS12, ou des connaissances/expériences équivalentes seraient bénéfiques.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Discuter des principes qui sous-tendent la création d'un programme de sécurité efficace à long terme. Interpréter le cadre de sécurité industrielle ISA/IEC 62443 et l'appliquer à votre activité
- Définir les bases des méthodologies d'analyse des risques et des vulnérabilités
- Décrire les principes du développement de la politique de sécurité
- Expliquer les concepts de défense en profondeur et les modèles de sécurité zone
- Analyser les tendances actuelles en matière d'incidents de sécurité industrielle et les méthodes utilisées par les pirates pour attaquer un système
- Définir les principes des principales techniques d'atténuation des risques, notamment les antivirus et la gestion des correctifs, les pare-feu et les réseaux privés virtuels

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION

Le prix de la certification est inclus dans le prix de la formation.

PROGRAMME

Comprendre l'environnement actuel de la sécurité industrielle : Qu'est-ce que la sécurité électronique pour les systèmes d'automatisation et de contrôle industriels ? | Les différences et les similitudes entre l'informatique et l'usine

Comment se produisent les cyberattaques : Comprendre les sources de la menace | Les étapes d'une cyberattaque réussie

Création d'un programme de sécurité : Facteurs critiques de réussite / Comprendre la norme ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009) - Sécurité des systèmes d'automatisation et de contrôle industriels : Établissement d'un programme de sécurité pour les systèmes d'automatisation et de contrôle industriels

Analyse des risques : Raison d'être de l'entreprise | Identification, classification et évaluation des risques

Gestion du risque par la politique, l'organisation et la sensibilisation à la sécurité : Portée du système de gestion de la cybersécurité | Sécurité organisationnelle | Formation et sensibilisation du personnel à la sécurité

Traiter le risque par des contre-mesures de sécurité sélectionnées : Sécurité du personnel | Sécurité physique et environnementale | Segmentation du réseau | Contrôle d'accès

Aborder le risque avec des mesures de mise en œuvre : Gestion et mise en œuvre des risques | Développement et maintenance des systèmes | Gestion de l'information et des documents

Surveillance et amélioration de l'IACS : Conformité et révision | Amélioration et maintenance de l'IACS

Valider ou vérifier la sécurité des systèmes : Que fait-on ? | Développer des produits et des systèmes sécurisés

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en anglais, formation dispensée en français-

KYRON

F-ISAAS-IC33

ISA/IEC 62443 CYBERSECURITY RISK ASSESSMENT SPECIALIST

FORMATION CERTIFIÉE

La première phase du cycle de vie de la cybersécurité de l'IACS (définie dans la norme ISA 62443-1-1) consiste à identifier et à documenter les actifs de l'IACS et à effectuer une évaluation de la vulnérabilité et des risques en matière de cybersécurité afin d'identifier et de comprendre les vulnérabilités à haut risque qui doivent être atténuées. Selon la norme ISA 62443-2-1, ces évaluations doivent être effectuées sur des applications nouvelles et sur des applications existantes. Une partie du processus d'évaluation consiste à développer un modèle de zone et de conduit du système, à identifier les cibles de niveau de sécurité et à documenter les exigences de cybersécurité dans une spécification des exigences de cybersécurité (CRS).

Ce cours fournira aux étudiants les informations et les compétences nécessaires pour évaluer la cybersécurité d'un IACS nouveau ou existant et pour développer une spécification des exigences de cybersécurité qui peut être utilisée pour documenter les exigences de cybersécurité du projet.

Mise à jour : Janvier 2024

PRÉREQUIS

Cours ISA IC32 ou connaissances/expérience équivalentes.

PUBLIC

- Ingénieurs et gestionnaires de systèmes de contrôle
- Intégrateurs de systèmes
- Ingénieurs et responsables informatiques des installations industrielles
- Professionnels de l'informatique d'entreprise/de la sécurité
- Sécurité des installations et gestion des risques

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Identifier et documenter le champ d'application de l'IACS
- Spécifier, rassembler ou générer les informations de cybersécurité requises pour réaliser l'évaluation
- Identifier ou découvrir les vulnérabilités en matière de cybersécurité inhérentes aux produits ou à la conception du système de l'IACS.
- Organiser et faciliter une évaluation des risques de cybersécurité pour un IACS
- Identifier et évaluer des scénarios de menaces réalistes
- Identifier les lacunes des politiques, procédures et normes existantes
- Établir et documenter les zones et les conduits de sécurité
- Préparer la documentation des résultats de l'évaluation

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION

Le prix de la certification est inclus dans le prix de la formation.

EXERCICES

- Critique des diagrammes d'architecture de système
- Inventaire des actifs
- Évaluation des écarts
- Évaluation des vulnérabilités de Windows
- Capture du trafic Ethernet
- Scan des ports
- Utilisation d'outils d'analyse des vulnérabilités
- Effectuer une évaluation des risques de haut niveau
- Créer un diagramme de zones et de conduits
- Effectuer une évaluation détaillée des risques de cybersécurité
- Critiquer une spécification des exigences de cybersécurité

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

PROGRAMME

Préparation d'une évaluation

Évaluation des vulnérabilités en matière de cybersécurité

Réalisation d'une évaluation des vulnérabilités

Évaluation des risques cyber

Réalisation d'une évaluation du risque cyber

Documentation et rapports

DURÉE
3 jours
(21 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en anglais, formation dispensée en français-

KYRON

F-ISADS-IC34

ISA/IEC 62443 CYBERSECURITY DESIGN SPECIALIST

FORMATION CERTIFIÉE

La deuxième phase du cycle de vie de la cybersécurité de l'IACS (définie dans la norme ISA 62443-1-1) porte sur les activités associées à la conception et à la mise en œuvre des contre-mesures de cybersécurité de l'IACS. Cela implique la sélection de contre-mesures appropriées en fonction de leur niveau de sécurité et de la nature des menaces et des vulnérabilités identifiées lors de la phase d'évaluation. Cette phase comprend également des tests d'acceptation de la cybersécurité de la solution intégrée, afin de valider que les contre-mesures sont correctement mises en œuvre et que l'IACS a atteint le niveau de sécurité cible.

Ce cours fournira aux étudiants les informations et les compétences nécessaires pour sélectionner et mettre en œuvre des contre-mesures de cybersécurité pour un IACS nouveau ou existant afin d'atteindre le niveau de sécurité cible attribué à chaque zone ou conduit de l'IACS. En outre, les étudiants apprendront à développer et à exécuter des plans de test pour vérifier que la cybersécurité d'une solution IACS a correctement satisfait aux objectifs de la spécification des exigences de cybersécurité.

Mise à jour : Janvier 2024

PUBLIC

- Ingénieurs et gestionnaires de systèmes de contrôle
- Intégrateurs de systèmes
- Ingénieurs et gestionnaires en informatique des installations industrielles
- Directeurs d'usine
- Sécurité des installations et gestion des risques

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Cours ISA IC32 et IC33 ou connaissances/expérience équivalentes.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Interpréter les résultats d'une évaluation des risques de cybersécurité d'un ICS
- Élaborer une spécification des besoins en matière de cybersécurité (CRS).
- Élaborer un modèle conceptuel sur la base des informations contenues dans une spécification des exigences de cybersécurité bien conçue.
- Expliquer le processus et les produits livrables du cycle de vie du développement de la sécurité
- Effectuer une configuration et une mise en service de base du pare-feu
- Concevoir une solution d'accès à distance sécurisée
- Développer une spécification de durcissement du système
- Mettre en œuvre un système de détection d'intrusion de réseau de base
- Élaboration d'un plan de test d'acceptation de la cybersécurité (CFAT/CSAT)

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION

Le prix de la certification est inclus dans le prix de la formation.

EXERCICES

- Build The Board
- Configurer les pare-feux et la DMZ
- Durcissement des dispositifs réseau
- Définir les politiques et les procédures
- Configuration de l'accès à distance
- Utiliser la norme 62443-3-3 pour valider les SL-A

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

PROGRAMME

Introduction au cycle de vie de la cybersécurité du ICS : Phase d'identification et d'évaluation, phase de conception et de mise en œuvre, phase d'exploitation et de maintenance

Processus de conception : Interprétation des résultats de l'évaluation des risques, spécifications des exigences de cybersécurité, développement d'une conception, spécifications de la conception

Processus de conception détaillée : Cycle de vie du développement de la sécurité (SDL), types de technologie, sélection de la technologie appropriée. Développement d'une conception détaillée, documentation de la conception/spécification

Exemples de conception et de mise en œuvre : Exemple de conception de pare-feu, exemple de conception d'accès à distance, exemple de conception de renforcement du système, exemple de conception de détection d'intrusion

Tests : Élaboration de plans de test, tests d'acceptation en usine de la cybersécurité, tests d'acceptation sur site de la cybersécurité

DURÉE
4 jours
(28 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

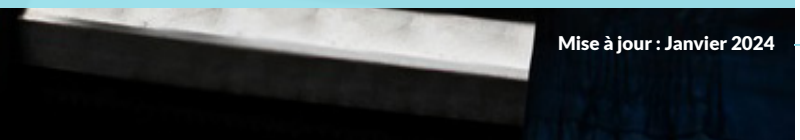
En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en anglais, formation dispensée en français-

KYRON

La troisième phase du cycle de vie de la cybersécurité IACS (définie dans la norme ISA 62443-1-1) se concentre sur les activités associées aux opérations et à la maintenance continues de la cybersécurité IACS. Cela implique le diagnostic et le dépannage du réseau, la surveillance de la sécurité et la réponse aux incidents, ainsi que la maintenance des contre-mesures de cybersécurité mises en œuvre dans la phase de conception et de mise en œuvre. Cette phase comprend également la gestion de la sécurité du changement, les procédures de sauvegarde et de récupération et les audits périodiques de cybersécurité.

Ce cours fournira aux étudiants les informations et les compétences nécessaires pour détecter et dépanner les événements potentiels de cybersécurité ainsi que les compétences nécessaires pour maintenir le niveau de sécurité d'un système d'exploitation tout au long de son cycle de vie malgré les défis d'un environnement de menaces en constante évolution.



Mise à jour : Janvier 2024

F-ISAMS-IC37

ISA/IEC 62443 CYBERSECURITY MAINTENANCE SPECIALIST

FORMATION CERTIFIÉE

PRÉREQUIS

Cours ISA TS06, TS12, TS20, IC32, IC33 et IC34 ou connaissances/expérience équivalentes

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

PUBLIC

- Personnel d'exploitation et de maintenance
- Ingénieurs et gestionnaires de systèmes de contrôle
- Intégrateurs de systèmes
- Ingénieurs et gestionnaires en informatique Installations industrielles
- Sécurité des installations et gestion des risques

OBJECTIFS - APTITUDE - COMPÉTENCES

- Effectuer un diagnostic et un dépannage de base du réseau
- Interpréter les résultats des alarmes de diagnostic des dispositifs IACS et des journaux d'événements.
- Mettre en œuvre les procédures de sauvegarde et de restauration IACS
- décrire le cycle de vie et la procédure de gestion des correctifs IACS
- Appliquer une procédure de gestion des antivirus
- Définir les principes de base du contrôle des applications et des outils de liste blanche.
- Définir les principes de base de la détection des intrusions dans les réseaux et les hôtes.
- Définir les principes de base des outils de surveillance des incidents et des événements de sécurité.
- Mettre en œuvre un plan de réponse aux incidents
- Mettre en œuvre une procédure de gestion du changement dans le cadre IACS
- Réaliser un audit de base de la cybersécurité IACS

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION

Le prix de la certification est inclus dans le prix de la formation.

EXERCICES

- Build The Board
- Gestion des correctifs
- Liste blanche
- Système de détection d'intrusion Snort
- Surveillance
- Versioning et sauvegardes
- Réaction aux incidents

Certificate 1 | Certificate 2 | Certificate 3 | Certificate 4 | Expert

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

PROGRAMME

Introduction au cycle de vie de la cybersécurité du ICS : Phase d'identification et d'évaluation, phase de conception et de mise en œuvre, phase d'exploitation et de maintenance

Diagnostic et dépannage du réseau : Interprétation des alarmes et des journaux d'événements des dispositifs, indicateurs précoces, systèmes de détection des intrusions dans le réseau, outils de gestion du réseau

Diagnostic et dépannage des applications : Interprétation des alarmes et des journaux d'événements du système d'exploitation et des applications, indicateurs précoces.
Outils de gestion des applications et de liste blanche, outils antivirus et de protection des points de terminaison, outils de surveillance des incidents et des événements de sécurité (SIEM)

Procédures et outils de cybersécurité IACS : Élaboration et suivi d'une procédure de gestion du changement IACS, Élaboration et suivi d'une procédure de sauvegarde IACS, Outils de gestion de la configuration IACS, Élaboration et suivi d'une procédure de gestion des correctifs IACS, Outils de gestion des correctifs, Élaboration et suivi d'une procédure de gestion des antivirus IACS, Outils de gestion des antivirus et de la liste blanche, Élaboration et suivi d'une procédure d'audit de cybersécurité IACS, Outils d'audit

Réponse aux incidents IACS : Élaborer et suivre un plan de réponse aux incidents IACS, enquête sur les incidents, récupération du système.

DURÉE
4 jours
(28 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

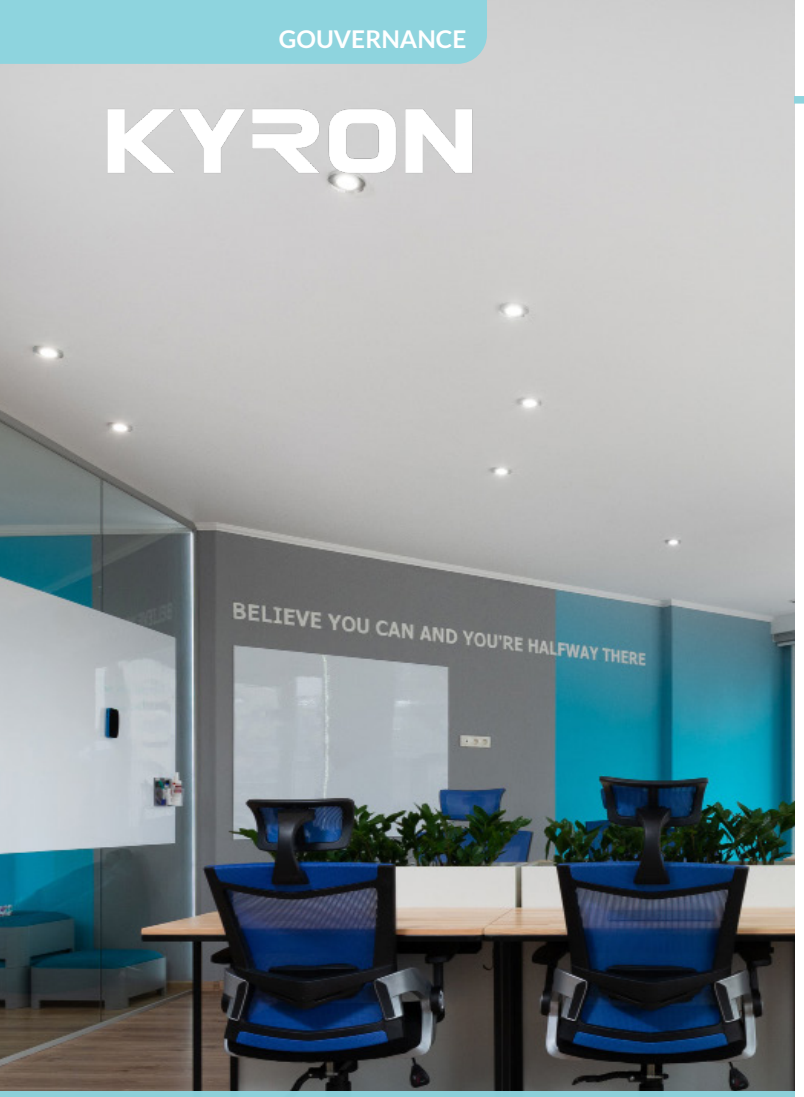
PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en anglais, formation dispensée en français-



INTRODUCTION AU SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION CONFORME À LA NORME ISO/IEC 27001

En participant à la formation d'introduction ISO/IEC 27001, vous allez comprendre l'importance d'un Système de management de la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27001IN

ISO 27001 INTRODUCTION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par le management de la sécurité de l'information ou souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Connaître les concepts, approches, méthodes et techniques permettant de mettre en œuvre un Système de management de la sécurité de l'information
- Comprendre les éléments fondamentaux d'un Système de management de la sécurité de l'information

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION

Aucune

PROGRAMME

Jour 1 : Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001

DURÉE
1 jour
(7 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

APPRÉHENDER LES BONNES PRATIQUES RELATIVES AUX MESURES DE SÉCURITÉ DE L'INFORMATION CONFORMES À LA NORME ISO/IEC 27002

La formation ISO/IEC 27001 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre et gérer un Système de management de la sécurité de l'information, selon la norme ISO 27001. Durant cette formation, vous apprendrez les différents modules d'un SMSI, y compris la politique SMSI, les procédures, la mesure de la performance, l'engagement de la direction, l'audit interne, la revue de la direction et l'amélioration continue.

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27001 Foundation ». La certification PECB Foundation atteste que vous avez compris les méthodes fondamentales, les exigences, le cadre et l'approche de management.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27001FO

ISO 27001 FOUNDATION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par le management de la sécurité de l'information, souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information ou souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Comprendre les éléments et le fonctionnement d'un Système de management de la sécurité de l'information
- Comprendre la corrélation entre la norme **ISO/IEC 27001 et ISO/IEC 27002** ainsi qu'avec d'autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management de la sécurité de l'information

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent postuler à la certification *PECB Certified ISO/IEC 27001 Foundation* via un Voucher qui sera transmis par mail. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
2 : Système de management de la sécurité de l'information

PROGRAMME

Jour 1 : Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001

Jour 2 : Exigences relatives au Système de management de la sécurité de l'information et préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISEZ LA MISE EN OEUVRE ET LA GESTION D'UN SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION (SMSI) CONFORME À LA NORME ISO/IEC 27001

La formation ISO/IEC 27001 Lead Implementer vous permettra 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/IEC 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/IEC 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/IEC 27001 dans une organisation.

Mise à jour : Janvier 2024

F-ISO27001LI

ISO 27001 LEAD IMPLEMENTER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

- Une bonne connaissance de la norme ISO/IEC 27001 et des connaissances approfondies des principes de mise en œuvre.
- Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Tout responsable ou consultant impliqué dans le management de la sécurité de l'information, conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information, responsables du maintien de la conformité aux exigences du SMSI ou membres d'une équipe du SMSI.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre la corrélation entre la norme **ISO/IEC 27001** et la norme **ISO/IEC 27002**, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme **ISO/IEC 27001** dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- 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

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

Les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27001 Provisional Implémenter* ou *Certified ISO/IEC 27001 Implementer* ou *Certified ISO/IEC 27001 Lead Implémenter* ou *Certified ISO/IEC 27001 Senior Lead Implémenter* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail. (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

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

PROGRAMME

Jour 1 : Introduction à ISO/IEC 27001 et initiation d'un SMSI
Objectifs et structure de la formation, normes et cadres réglementaires, système de management de la sécurité de l'information (SMSI), concepts et principes fondamentaux de la sécurité de l'information, Initiation de la mise en œuvre du SMSI, compréhension de l'organisme et de son contexte, périmètre du SMSI

Jour 2 : Planification de la mise en œuvre d'un SMSI
Leadership et approbation du projet, structure organisationnelle, analyse du système existant, politique de sécurité de l'information, gestion des risques, déclaration d'applicabilité

Jour 3 : Mise en œuvre d'un SMSI
Gestion de l'information documentée, sélection et conception des mesures de sécurité, mise en œuvre des mesures de sécurité, tendances et technologies, communication, compétence et sensibilisation, gestion des opérations de sécurité

Jour 4 : Surveillance du SMSI, amélioration continue et préparation à l'audit de certification
Surveillance, mesure, analyse et évaluation, audit interne, revue de direction, traitement des non-conformités, amélioration continue, préparation à l'audit de certification, processus de certification et clôture de la formation

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISEZ L'AUDIT D'UN SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION (SMSI) CONFORME À LA NORME ISO/IEC 27001

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 27701 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.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27001LA

ISO 27001 LEAD AUDITOR

PUBLIC

Toute personne intéressée par le management de la sécurité de l'information, souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information ou souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Une bonne connaissance de la norme ISO/IEC 27001 et des connaissances approfondies sur les principes de l'audit.
Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme **ISO/IEC 27001**
- Expliquer la corrélation entre la norme **ISO/IEC 27001** et la norme **ISO/IEC 27002,** ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme **ISO 19011**
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'**ISO/IEC 27001** dans le contexte d'un audit du SMSI
- 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**

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

Les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27001 Provisional Auditor* ou *Certified ISO/IEC 27001 Auditor* ou *Certified ISO/IEC 27001 Lead Auditor* ou *Certified ISO/IEC 27001 Senior Lead Auditor* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail. (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

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

PROGRAMME

Jour 1 : **Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001**
Objectifs et structure de la formation, normes et cadres réglementaires, processus de certification, concepts et principes fondamentaux de la sécurité de l'information, système de management de la sécurité de l'information (SMSI)
Jour 2 : **Principes d'audit, préparation et initiation d'un audit**
Concepts et principes fondamentaux de l'audit, impact des tendances et de la technologie en audit, audit basé sur les preuves, audit basé sur les risques, initiation du processus d'audit, étape 12 de l'audit
Jour 3 : **Activités d'audit sur site**
Préparation de l'étape 2 de l'audit, étape 2 de l'audit, communication pendant l'audit, procédures d'audit, création de plans d'échantillonnage d'audit
Jour 4 : **Clôture de l'audit**
Rédaction des rapports de constatations d'audit et de non-conformité, documentation d'audit et revue de la qualité, clôture de l'audit, évaluation des plans d'action par l'auditeur, après l'audit initial, gestion d'un programme d'audit interne
Jour 5 : **Préparation à l'examen de certification**

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

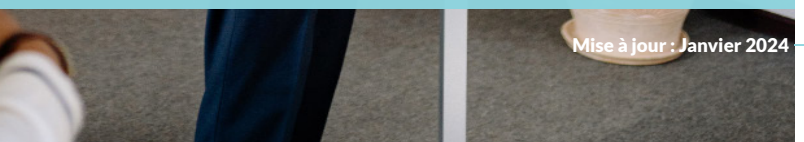
-Support en français, formation dispensée en français-

KYRON

INTRODUCTION AUX MESURES DE SÉCURITÉ DE L'INFORMATION, CONFORMES À LA NORME ISO/IEC 27002

La formation d'introduction à la norme ISO/IEC 27002 vous permettra d'appréhender les systèmes de management de la sécurité de l'information et les mesures de sécurité de l'information telles que définies par la norme ISO/IEC 27002.

En participant à la formation d'introduction ISO/IEC 27002, vous allez comprendre l'importance d'un SMSI et des mesures de la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.



Mise à jour : Janvier 2024

F-ISO27002IN

ISO 27002 INTRODUCTION

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Aucun

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne intéressée par le management de la sécurité de l'information et les mesures de sécurité de l'information et les personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Connaître les normes relatives à la sécurité de l'information et les bonnes pratiques de management de la sécurité de l'information permettant de mettre en œuvre et de gérer les mesures de la sécurité de l'information
- Comprendre les mesures de sécurité nécessaires pour gérer les risques de la sécurité de l'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION

Aucune

PROGRAMME

Jour 1 : Introduction aux mesures de sécurité de l'information, telles que définies par la norme ISO/IEC 27002

DURÉE
1 jour
(7 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

APPRÉHENDER LES BONNES PRATIQUES RELATIVES AUX MESURES DE SÉCURITÉ DE L'INFORMATION CONFORMES À LA NORME ISO/IEC 27002

La formation ISO/IEC 27002 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre les mesures de sécurité de l'information, selon la norme ISO/IEC 27002.

Durant cette formation, vous apprendrez comment l'ISO/IEC 27001 et l'ISO/IEC 27002 sont correspondantes à l'ISO/IEC 27003 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information), ISO/IEC 27004 (Management de la sécurité de l'information - Surveillance, mesurage, analyse et évaluation) et ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information).

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27002 Foundation ». La certification PECB Foundation atteste que vous avez compris les méthodes fondamentales et l'approche de management.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27002FO

ISO 27002 FOUNDATION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par le management de la sécurité l'information et les mesures de la sécurité de l'information, souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information ou souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Comprendre la mise en œuvre des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002
- Comprendre la corrélation entre les normes ISO/IEC 27001 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *PECB Certified ISO/IEC 27002 Foundation*. via un Voucher qui sera transmis par mail. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
2 : Système de management de la sécurité de l'information conformes à la norme ISO/IEC 27002

PROGRAMME

Jour 1 : Introduction à la norme ISO/IEC 27002 et au Système de management de la sécurité de l'information

Jour 2 : Mesures ISO/IEC 27002 et préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

COMPRENDRE LA MISE EN ŒUVRE ET LA GESTION DES MESURES DE SÉCURITÉ DE L'INFORMATION CONFORMES À LA NORME ISO/IEC 27002

La formation ISO/IEC 27002 Manager vous permettra d'acquérir l'expertise nécessaire pour soutenir une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002. Durant cette formation, vous acquerrez également une compréhension approfondie sur les meilleures pratiques en matière de mesures de la sécurité d'information.

Après avoir appréhendé tous les concepts nécessaires des mesures de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27002 Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et les compétences professionnelles pour mettre en œuvre et gérer les mesures de la sécurité d'information dans une organisation.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27002MA

ISO 27002 MANAGER

PRÉREQUIS

Des connaissances fondamentales de la norme ISO/IEC 27002 et des connaissances approfondies sur la sécurité de l'information. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Responsables ou consultants désirant mettre en œuvre un système de management de la sécurité de l'information (SMSI) conforme aux normes ISO/IEC 27001 et ISO/IEC 27002. Tout individu responsable de la sécurité d'information dans une organisation, les membres de l'équipe de sécurité de l'information. Conseillers spécialisés en technologies de l'information, professionnels des TI et agents de la protection des données personnelles et de la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre la corrélation entre la norme **ISO/IEC 27002** et la norme **ISO/IEC 27001**
- Comprendre la mise en œuvre des mesures de sécurité d'information en conformité avec la norme **ISO/IEC 27002**
- Développer l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de sécurité d'information
- Comprendre la formulation et la mise en œuvre des exigences et des objectifs de la sécurité d'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27002 Provisional Manager* ou *Certified ISO/IEC 27002 Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies).

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux de la sécurité de l'information
2 : Mesures de la sécurité de l'information conformes à la norme ISO/IEC 27002

PROGRAMME

Jour 1 : Introduction aux mesures de sécurité d'information selon la norme ISO/IEC 27002
Objectifs et structure de la formation, cadres normatifs et réglementaires, principes fondamentaux de la sécurité de l'information, système de management de la sécurité de l'information, politiques de sécurité de l'information, management de la sécurité de l'information
Jour 2 : Exigences et objectifs de la sécurité de l'information conforme à la norme ISO/IEC 27002
Gestion des actifs, contrôle d'accès, cryptographie, sécurité physique et environnementale, sécurité liée à l'exploitation
Jour 3 : Surveiller, mesurer, analyser et évaluer les mesures de la sécurité de l'information et préparation à l'examen de certification
Sécurité des communications, acquisition, développement et maintenance des systèmes d'information, relations avec les fournisseurs, gestion des incidents liés à la sécurité de l'information, aspects de la sécurité de l'information dans la gestion de la continuité de l'activité, conformité, compétences et évaluation des gestionnaires, préparation à l'examen de certification

DURÉE
3 jours
(21 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISEZ LA MISE EN ŒUVRE ET LA GESTION DES MESURES DE SÉCURITÉ DE L'INFORMATION CONFORMES À LA NORME L'ISO/IEC 27002

La formation ISO/IEC 27002 Lead Manager vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002. Durant cette formation, vous acquerrez des connaissances approfondies sur les meilleures pratiques en matière de mesures de sécurité de l'information et vous serez apte à améliorer la sécurité de l'information dans une organisation.

Après avoir maîtrisé l'ensemble des concepts relatifs aux mesures de sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27002 Lead Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger une équipe dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002.

Mise à jour : Janvier 2024

F-ISO27002LM

ISO 27002 LEAD MANAGER

FORMATION CERTIFIÉE PECB

PUBLIC

Responsables ou consultants désirant mettre en œuvre un système de management de la sécurité de l'information (SMSI) conforme aux normes 27001 et ISO/IEC 27002, chefs des projets ou consultants souhaitant maîtriser les processus de mise en œuvre du système de management de la sécurité de l'information. Toute personne responsable de la sécurité de l'information, de la conformité, du risque et de la gouvernance dans une organisation, membres de l'équipe de la sécurité de l'information et agents de la protection des données personnelles.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Une bonne connaissance de la norme ISO/IEC 27001 et des connaissances approfondies des principes de mise en œuvre. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/IEC 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion effcace des mesures de la sécurité de l'information
- Comprendre la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Comprendre l'importance de la sécurité de l'information pour la stratégie de l'organisation
- Maîtriser la mise en œuvre des processus de la sécurité de l'information
- Maîtriser l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information
- Maîtriser la formulation et la mise en œuvre des exigences et des objectifs de la sécurité de l'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27002 Provisional Manager* ou *Certified ISO/IEC 27002 Manager* ou *Certified ISO/IEC 27002 Lead Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux de la sécurité de l'information
2 : Mesures de la sécurité de l'information conformes à la norme ISO/IEC 27002
3 : Planification et évaluation des besoins et applicabilité des mesures de la sécurité d'information
4 : Mise en œuvre et management des mesures de la sécurité de l'information
5 : Surveillance et mesure des mesures de la sécurité de l'information
6 : Amélioration continue des mesures de la sécurité de l'information

PROGRAMME

Jour 1 : Introduction aux mesures de sécurité de l'information conformes à la norme l'ISO/IEC 27002
Objectifs et structure de la formation, cadres normatifs et réglementaires, principes fondamentaux de la sécurité de l'information, système de management de la sécurité de l'information, politiques de sécurité de l'information, management de la sécurité de l'information
Jour 2 : Exigences et objectifs de la sécurité de l'information conforme à la norme ISO/IEC 27002
Sécurité des ressources humaines, gestion des actifs, contrôle d'accès
Jour 3 : Surveiller, mesurer, analyser et évaluer les mesures de la sécurité de l'information
Cryptographie, sécurité physique et environnementale, sécurité liée à l'exploitation, sécurité des communications
Jour 4 : Amélioration continue de la performance du Système de management de la sécurité de l'information de l'organisation
Acquisition, développement et maintenance des systèmes d'information, relations avec les fournisseurs, gestion des incidents liés à la sécurité de l'information, aspects de la sécurité de l'information dans la gestion de la continuité de l'activité, conformité, compétences et évaluation des gestionnaires, clôture de la formation
Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

LA FORMATION ISO/IEC 27032 FOUNDATION PRÉSENTE LES CONCEPTS ET PRINCIPES FONDAMENTAUX DE LA CYBERSÉCURITÉ BASÉS SUR L'ISO/IEC 27032 ET LE CADRE DE CYBERSÉCURITÉ DU NIST

L'essor du cyberespace pendant la révolution numérique a par conséquent donné naissance aux cybermenaces et à la cybersécurité. Le cours de formation ISO/IEC 27032 Foundation présente les principaux concepts et exigences d'un programme de cybersécurité, notamment les parties prenantes du cyberespace, les mécanismes d'attaque, ainsi que le partage et la coordination des informations.

Le cours de formation est suivi de l'examen de certification. Si vous le réussissez, vous pouvez demander le titre de "Certifié PECB ISO/IEC 27032 Foundation", qui démontre votre connaissance des concepts, principes et techniques fondamentaux de la cybersécurité.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27032FO

ISO 27032 FOUNDATION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne impliquée dans la cybersécurité et la sécurité de l'information, intéressée par le domaine de la cybersécurité ou souhaitant poursuivre une carrière dans la cybersécurité.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Comprendre les concepts et principes de base de la cybersécurité
- Reconnaître la corrélation entre la norme **ISO/IEC 27032**, le cadre de cybersécurité du NIST et d'autres normes et cadres
- **Comprendre les approches, les méthodes et les techniques utilisées dans le domaine de la cybersécurité**

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27032 Foundation* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux de la cybersécurité
2 : Programme de cybersécurité

PROGRAMME

Jour 1 : Introduction à la norme ISO/IEC 27032 et aux principes fondamentaux principes et concepts de cybersécurité

Jour 2 : Cybersecurity program et préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISER LA MISE EN ŒUVRE ET LE MANAGEMENT D'UN PROGRAMME DE CYBERSÉCURITÉ BASÉ SUR LA NORME ISO/IEC 27032

La norme ISO/IEC 27032 fait référence à la « cybersécurité » ou à la « sécurité du cyberespace », qui est définie comme la protection de la vie privée, de l'intégrité et de l'accessibilité des données dans le cyberespace. Par conséquent, le cyberespace est reconnu comme une interaction de personnes, de logiciels et de services technologiques mondiaux.

La norme internationale ISO/IEC 27032 vise à mettre l'accent sur le rôle des différentes sécurités dans le cyberespace, au regard de la sécurité de l'information, de la sécurité des réseaux et de l'Internet et de la protection des infrastructures d'information essentielles.
L'ISO/IEC 27032 fournit un cadre stratégique pour traiter la question de la confiance, de la collaboration et de l'échange d'informations ainsi que des conseils techniques pour l'intégration des systèmes entre les parties prenantes du cyberespace.

Mise à jour : Janvier 2024

F-ISO27032LM

ISO 27032 LEAD CYBERSECURITY MANAGER

FORMATION CERTIFIÉE PECB

PUBLIC

Professionnels de la cybersécurité et des TI souhaitant accroître leurs connaissances et compétences techniques ou souhaitant gérer un programme de cybersécurité, experts en sécurité de l'information, responsables du développement d'un programme de cybersécurité, spécialistes des TI et conseillers spécialisés dans les TI.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Une connaissance fondamentale sur la norme ISO/IEC 27032 et des connaissances approfondies sur la cybersécurité. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'**ISO/IEC 27032** et le Cadre de Cybersécurité **NIST**
- Connaître l'objectif, le contenu et la corrélation entre **l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST** ainsi qu'avec d'autres normes et cadres opérationnels
- Maîtriser les concepts, les approches, les normes, les méthodes et les techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation
- Savoir interpréter les lignes directrices de l'**ISO/IEC 27032** dans le contexte spécifique d'une organisation
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans **l'ISO/IEC 27032** et le cadre de **Cybersécurité NIST**
- Maîtriser les compétences pour conseiller une organisation sur les bonnes pratiques de gestion de la cybersécurité

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27032 Provisional Cybersecurity Manager* ou *Certified ISO/IEC 27032 Cybersecurity Manager* ou *Certified ISO/IEC 27032 Lead Cybersecurity Manager* ou *Certified ISO/IEC 27032 Senior Lead Cybersecurity Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail. (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

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

PROGRAMME

Jour 1 : Introduction à la cybersécurité et aux concepts connexes, tels que définis par l'ISO/IEC 27032
Objectifs et structure du cours, normes et cadres réglementaires, notions fondamentales de la cybersécurité, programme de cybersécurité. lancer un programme de cybersécurité, analyser l'organisme, leadership

Jour 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaque
Politiques de cybersécurité, gestion du risque de la cybersécurité, mécanismes d'attaque

Jour 3 : Contrôles en cybersécurité, partage des informations et coordination
Mesures de contrôle de cybersécurité, partage et coordination de l'information, programme de formation et de sensibilisation

Jour 4 : Gestion des incidents, suivi et amélioration continue
Continuité des activités, management des incidents de cybersécurité, Intervention et récupération en cas d'incident de cybersécurité, tests en cybersécurité, mesure de la performance, amélioration continue

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

SE FAMILIARISER AVEC LES CONCEPTS DE BASE ET LES EXIGENCES DU MODÈLE CMMC

La formation PECB CMMC Foundations vous permet d'en savoir plus sur la structure du modèle CMMC, notamment les niveaux, les domaines, les capacités, les processus et les pratiques CMMC. Vous acquerrez également des connaissances de base liées à l'écosystème CMMC, au processus et à la méthodologie d'évaluation CMMC ainsi qu'au Code de déontologie CMMC.

La formation est suivie d'un examen. La certification PECB Foundations est le signe que vous comprenez le modèle CMMC, que vous êtes capable d'interpréter les exigences des niveaux CMMC spécifiques et que vous avez les connaissances de base pour aider un organisme à mettre en œuvre et à gérer les exigences du modèle CMMC.

Mise à jour : Janvier 2024

F-CMMC-FO

CYBERSECURITY MATURITY MODEL CERTIFICATION FOUNDATION

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Aucun

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne souhaitant faire partie de l'écosystème CMMC ou cherchant à acquérir des connaissances sur le modèle CMMC ou toute personne intéressée par l'utilisation du modèle CMMC. Les fournisseurs du ministère de la Défense (DoD) et de la base industrielle de la Défense (DIB) et aux autres personnes souhaitant obtenir la certification CMMC.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre les concepts de base, les définitions et les approches du modèle **CMMC**
- Vous familiariser avec les niveaux de maturité, les domaines, les processus et les pratiques **CMMC**
- Développer une compréhension générale de la manière dont le modèle **CMMC** pourrait être appliqué dans la chaîne d'approvisionnement **du DoD et du secteur DIB**

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified CMMC Foundations* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Concepts fondamentaux du modèle CMMC, de l'écosystème CMMC et du code de déontologie.
2 : Domaines, processus, pratiques et processus d'évaluation CMMC

PROGRAMME

Jour 1 : Introduction à l'écosystème CMMC et au modèle CMMC

Jour 2 : Pratiques CMMC, processus d'évaluation et code de déontologie

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

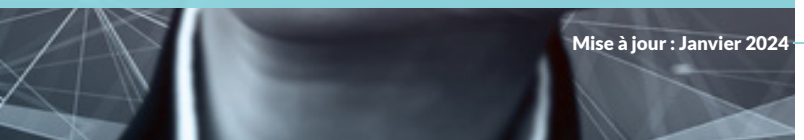
En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

MAÎTRISER LES CONCEPTS ET LES EXIGENCES DES NIVEAUX, DOMAINES, CAPACITÉS, PROCESSUS ET PRATIQUES DU CMMC, LES PHASES DE LA MÉTHODOLOGIE D'ÉVALUATION DU CMMC ET L'ÉCOSYSTÈME DU CMMC-AB

En suivant la formation CMMC-AB Certified Professional, vous acquerrez des connaissances sur la structure du modèle CMMC, notamment les niveaux, les domaines, les capacités, les processus et les pratiques CMMC. En outre, vous développerez votre capacité à comprendre, différencier et expliquer la relation entre le CMMC et la documentation de référence primaire telle que le FAR 52.204-21, le DFARS 252.204-7012, le DFARS 252.204-7019-7021, le NIST SP 800-171, le NIST 800-172, le NIST 800-53, les définitions et directives en matière de CUI (informations contrôlées non classifiées) du NARA et du DOD, et le CERT RMM. Vous pourrez également (a) identifier, décrire et comparer les rôles et les responsabilités de chaque membre de l'écosystème CMMC-AB ; (b) connaître les phases de la méthodologie d'évaluation CMMC ; (c) identifier et atténuer les problèmes d'éthique en vous appuyant sur le Code de déontologie CMMC-AB ; et (d) définir et déterminer les rôles et responsabilités en ce qui concerne les informations des contrats fédéraux (FCI) et les informations contrôlées non classifiées (CUI).

Cette formation vous permettra de devenir un atout précieux pour les agences de conseil, les organismes d'évaluateurs tiers du CMMC (C3PAO) et les organismes qui demandent des ressources formées CMMC.



Mise à jour : Janvier 2024

F-CMMC-PRO

CYBERSECURITY MATURITY MODEL CERTIFICATION CERTIFIED PROFESSIONAL

FORMATION CERTIFIÉE PECB

PUBLIC

Toute personne qui souhaite faire partie de l'écosystème CMMC-AB telles que les évaluateurs certifiés et les instructeurs certifiés, qui cherche à acquérir des connaissances sur le modèle CMMC et ses exigences, qui souhaite fournir des services de conseil pour la préparation du CMMC ou toute personne travaillant pour les fournisseurs du ministère de la Défense (DoD) et la base industrielle de la Défense (DIB) et pour d'autres organismes souhaitant obtenir la certification CMMC et les consultants en cybersécurité et en technologie et membres de l'équipe d'évaluation CMMC.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Il est recommandé d'avoir une connaissance générale des concepts et principes de la cybersécurité et des technologies de l'information. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Avoir une connaissance complète des domaines, des capacités, des niveaux, des processus et des pratiques du modèle CMMC
- Reconnaître la corrélation entre le modèle **CMMC, la clause 52.204-21 du FAR, la clause 252.204-7012 du DFARS, le NIST SP 800-171** et d'autres normes et cadres
- Acquérir la capacité d'interpréter les exigences du modèle **CMMC** dans le contexte spécifique d'un organisme en quête de certification **(OSC)**
- Obtenir les connaissances nécessaires pour aider un organisme à mettre en œuvre et à gérer efficacement les exigences du modèle **CMMC** pour le niveau **CMMC** requis
- Acquérir des connaissances sur la méthodologie et le processus d'évaluation du modèle **CMMC**

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified CMMC Foundations* ou *CMMC-AB Certified Professional* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies).

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Sources de données et gouvernance
2 : Écosystème CMMC-AB
3 : Éthique
4 : Modèle CMMC
5 : Mise en œuvre CMMC

PROGRAMME

Jour 1 : Introduction aux parties prenantes, au modèle et aux pratiques CMMC de niveau 1

Jour 2 : Processus et pratiques CMMC des niveaux 2 et 3

Jour 3 : Processus et pratiques CMMC des niveaux 4 et 5

Jour 4 : Rôles et responsabilités, éthique et méthodologie d'évaluation de l'écosystème CMMC-AB

DURÉE
4 jours
(28 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

INTRODUCTION AUX MESURES DE SÉCURITÉ DE L'INFORMATION, CONFORMES À LA NORME ISO/IEC 27002

La formation d'introduction à la norme ISO/IEC 27002 vous permettra d'appréhender les systèmes de management de la sécurité de l'information et les mesures de sécurité de l'information telles que définies par la norme ISO/IEC 27002.

En participant à la formation d'introduction ISO/IEC 27002, vous allez comprendre l'importance d'un SMSI et des mesures de la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO27005IN

ISO 27005 INTRODUCTION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par la gestion des risques liés à la sécurité de l'information et souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Connaître les concepts, approches, méthodes et techniques permettant de gérer les risques liés à la sécurité de l'information
- Comprendre l'importance de la gestion des risques liés à la sécurité de l'information

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION

Aucune

PROGRAMME

Jour 1 : **Introduction aux fondamentaux de la gestion des risques liés à la sécurité de l'information en utilisant la norme ISO/IEC 27005**

DURÉE
1 jour
(7 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

APPRÉHENDER LES BONNES PRATIQUES RELATIVES AUX MESURES DE SÉCURITÉ DE L'INFORMATION CONFORMES À LA NORME ISO/IEC 27002

La formation ISO/IEC 27002 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre les mesures de sécurité de l'information, selon la norme ISO/IEC 27002.

Durant cette formation, vous apprendrez comment l'ISO/IEC 27001 et l'ISO/IEC 27002 sont correspondantes à l'ISO/IEC 27003 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information), ISO/IEC 27004 (Management de la sécurité de l'information - Surveillance, mesurage, analyse et évaluation) et ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information).

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27002 Foundation ». La certification PECB Foundation atteste que vous avez compris les méthodes fondamentales et l'approche de management.

Mise à jour : Janvier 2024

F-ISO27005FO

ISO 27005 FOUNDATION

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Aucun

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne concernée par la gestion des risques liés à la sécurité de l'information, souhaitant acquérir des connaissances relatives aux principaux processus de la gestion des risques liés à la sécurité de l'information et poursuivre une carrière dans la gestion des risques liés à la sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre les concepts de gestion des risques liés à la sécurité de l'information, conforme à la norme **ISO/IEC 27005**
- Comprendre la corrélation entre la norme **ISO/IEC 27005** et les autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de gérer des risques liés à la sécurité de l'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/CEI 27005 Foundation* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information
2 : Approches et processus de gestion des risques en sécurité de l'information

PROGRAMME

Jour 1 : Introduction aux concepts fondamentaux de la gestion des risques liés à la sécurité de l'information en utilisant la norme ISO/IEC 27005

Jour 2 : Approches de gestion des risques liés à la sécurité de l'information, préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

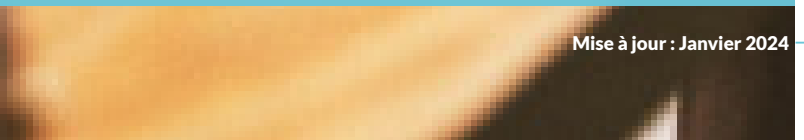
En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

MAÎTRISEZ LES PRINCIPES ET LES CONCEPTS FONDAMENTAUX DE L'APPRÉCIATION DES RISQUES ET DE LA GESTION OPTIMALE DES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION CONFORMÉMENT À LA NORME ISO/IEC 27005

La formation « ISO/IEC 27005 Risk Manager » vous permettra 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.

Après avoir compris tous les concepts nécessaires du management du risque de la sécurité de l'information basé sur la norme ISO/IEC 27005, vous pouvez vous présenter à l'examen et demander une certification "PECB Certified ISO/IEC 27005 Risk Manager". En détenant un certificat PECB Risk Manager, vous serez en mesure de démontrer que vous avez les compétences et les connaissances nécessaires pour effectuer une évaluation optimale des risques de sécurité de l'information et gérer les risques de sécurité de l'information dans les délais impartis.



Mise à jour : Janvier 2024

F-ISO27005RM

ISO 27005 RISK MANAGER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Une compréhension fondamentale de la norme ISO/IEC 27005 et une connaissance approfondie de l'évaluation des risques et de la sécurité de l'information. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Tout individu responsable de la sécurité d'information, de la conformité et du risque dans un organisme ou mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de management du risque. Tous les responsables de la sécurité d'information, membres d'une équipe de sécurité de l'information, consultants et professionnels des TI et les agents de la sécurité de l'information et de la protection de la vie privée.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à **ISO/IEC 27005**
- Savoir interpréter les exigences de la norme **ISO/IEC 27001** dans le cadre du management du risque de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(2h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27005 Provisional Risk Manager* ou *Certified ISO/IEC 27005 Risk Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information

2 : Mettre en œuvre un programme de gestion des risques liés à la sécurité de l'information

3 : Processus et cadre de gestion des risques liés à la sécurité de l'information conformes à la norme ISO/IEC 27005

4 : Autres méthodes d'appréciation des risques de la sécurité de l'information

PROGRAMME

Jour 1 : Introduction au programme de gestion des risques conforme à ISO/IEC 27005

Objectifs et structure de la formation, cadres normatifs et réglementaires, concepts et définition du risque, programme de gestion des risques, établissement du contexte

Jour 2 : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005

Identification des risques, analyse et évaluation des risques, appréciation du risque avec une méthode quantitative, traitement des risques, acceptation des risques et gestion des risques résiduels, communication relative aux risques, surveillance et réexamen des risques

Jour 3 : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et préparation à l'examen de certification

Méthode OCTAVE, méthode MEHARI, méthode EBIOS, méthode harmonisée d'EMR

DURÉE
3 jours
(21 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

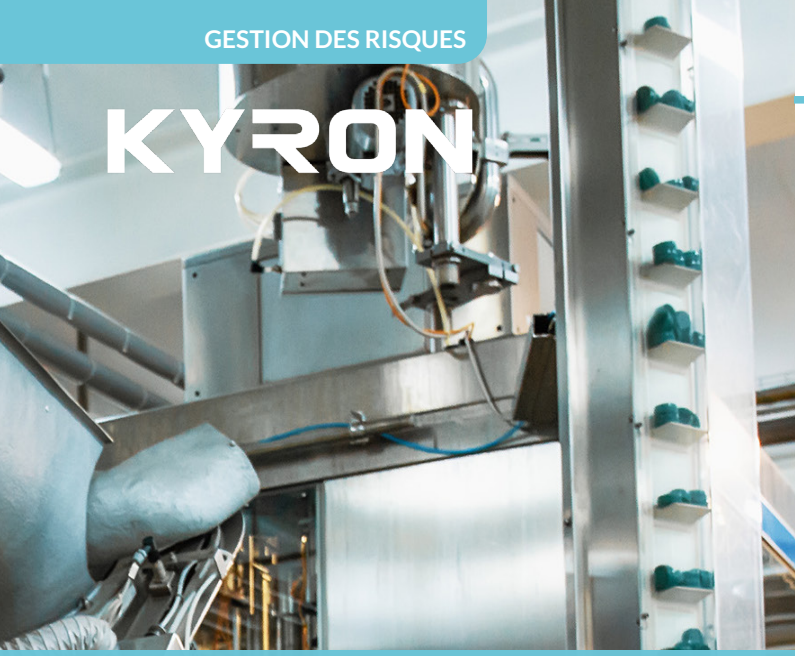
PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-



KYRON

DÉVELOPPER LES COMPÉTENCES NÉCESSAIRES POUR EFFECTUER UNE ÉVALUATION DES RISQUES À L'AIDE DE LA MÉTHODE EBIOS.

La formation EBIOS Risk Manager vous permet d'acquérir les connaissances et de développer les compétences nécessaires pour maîtriser les concepts et les composantes de la gestion des risques liés à tous les actifs pertinents pour la sécurité de l'information selon la méthode EBIOS.

Sur la base d'exercices pratiques et d'études de cas, vous aurez l'occasion d'acquérir les compétences nécessaires pour réaliser une évaluation optimale des risques liés à la sécurité de l'information et une gestion opportune des risques en se familiarisant avec son cycle de vie. Cette formation s'inscrit parfaitement dans le cadre du processus de mise en œuvre de la norme ISO/IEC 27001.

Après avoir maîtrisé tous les concepts nécessaires à l'évaluation des risques à l'aide de la méthode EBIOS, vous pourrez passer l'examen et postuler pour obtenir un titre de "Risk Manager EBIOS certifié PECB". En détenant un certificat PECB Risk Manager, vous pourrez démontrer que vous possédez les connaissances pratiques et les capacités professionnelles pour aider une organisation à effectuer une évaluation des risques basée sur la méthode EBIOS.

Mise à jour : Janvier 2024

F-METHEBIOS

RISK MANAGER MÉTHODE EBIOS

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Des connaissances de base en cybersécurité et réseaux informatiques sont requises

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnes 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

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la **méthode EBIOS**
- Comprendre les étapes de la **méthode EBIOS** afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Comprendre et expliquer les résultats d'une étude **EBIOS** et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude **EBIOS**
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(2,5h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *PECB Certified EBIOS Risk Manager* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information selon la méthode EBIOS
2 : Programme de gestion des risques liés à la sécurité de l'information basée sur EBIOS
3 : Appréciation des risques liés à la sécurité de l'information basée sur la méthode EBIOS

PROGRAMME

Jour 1 : Introduction à la méthode EBIOS
Cadrage et socle de sécurité, sources de risque
Jour 2 : Développement méthode EBIOS
Scénarios stratégiques, scénarios opérationnels, traitement du risque, processus de certification
Jour 3 : Préparation à l'examen final

DURÉE
3 jours
(21 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

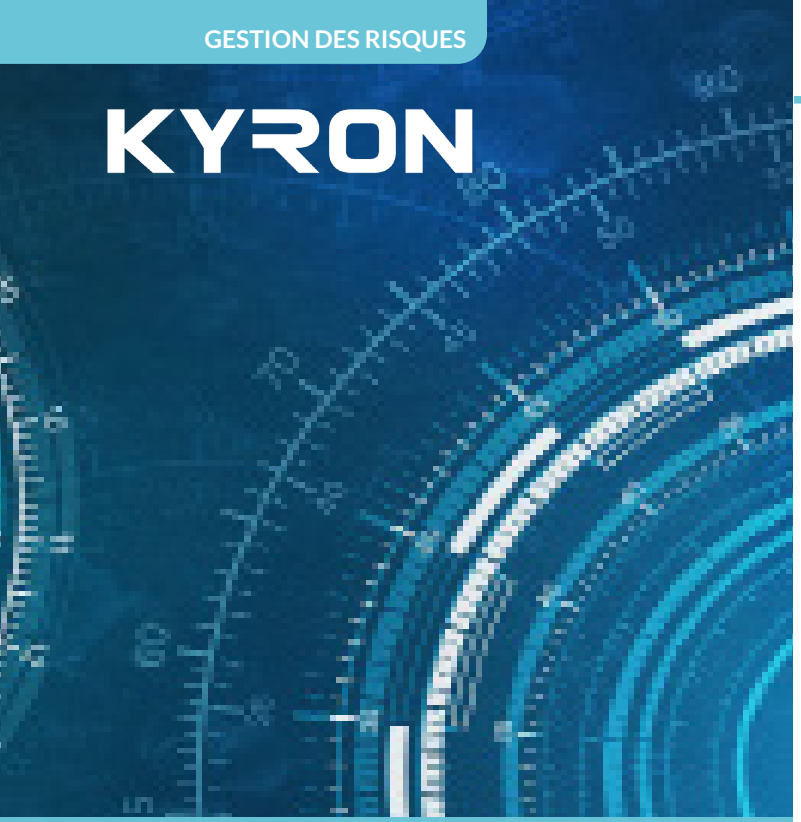
DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON



La formation MEHARI vous permettra d'acquérir l'expertise et les connaissances nécessaires pour analyser les risques liés à la sécurité de l'information inclus dans différentes étapes du cycle de vie de la sécurité dans un organisme. Cette formation est conçue de manière à vous doter des compétences nécessaires pour examiner les services de sécurité, détecter les risques critiques et analyser les scénarios de risque en conformité avec la méthode d'analyse des risques MEHARI.

Grâce à une formation basée sur des exercices pratiques et des études de cas, vous acquerrez les compétences nécessaires pour réaliser une analyse et une classification des enjeux, évaluer les services de sécurité, mener une analyse du risque et définir les plans de sécurité.

Après avoir maîtrisé l'ensemble des concepts relatifs à l'analyse des risques à l'aide de la méthode MEHARI, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified MEHARI Risk Manager ». En étant titulaire d'une certification PECB Risk Manager, vous démontrerez que vous disposez des connaissances pratiques et des capacités professionnelles nécessaires pour aider un organisme à mener une appréciation des risques basée sur la méthode MEHARI.

Mise à jour : Janvier 2024

F-METHMEHARI

RISK MANAGER MÉTHODE MEHARI

FORMATION CERTIFIÉE PECB

PUBLIC

Toute personne souhaitant acquérir des connaissances approfondies sur la méthode d'analyse et le modèle de risque de MEHARI, les gestionnaires désirant développer les compétences nécessaires pour soutenir les organismes en matière d'analyse du risque lié à la sécurité de l'information, les auditeurs souhaitant acquérir une connaissance approfondie de la méthode MEHARI et les membres d'une équipe de sécurité de l'information souhaitant améliorer leurs compétences et maîtriser l'évaluation de la qualité des services de sécurité.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PRÉREQUIS

Une connaissance en management des risques est recommandée. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre les concepts et les principes généraux associés à la méthode d'analyse des risques **MEHARI**
- Acquérir une compréhension approfondie des quatre étapes de l'approche **MEHARI**
- Développer les compétences nécessaires pour identifier les dysfonctionnements, analyser les scénarios de chaque dysfonctionnement, identifier l'échelle de la valeur des dysfonctionnements et préparer une classification formelle des actifs du système d'information
- Développer les compétences nécessaires pour évaluer la qualité des services de sécurité dans un organisme à l'aide de la méthode **MEHARI**
- Comprendre le modèle de risque **MEHARI**
- Développer les compétences nécessaires pour définir les risques, analyser les situations de risque et réaliser une analyse quantitative d'une situation de risque
- Acquérir les compétences nécessaires pour élaborer des plans de sécurité basés sur l'approche **MEHARI**

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(2h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *PECB Certified ISO/IEC 27005 EBIOS Risk Manager* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux de la méthode MEHARI relative à l'analyse des risques
2 : Analyse des enjeux et classification
3 : Analyse du risque
4 : Définition de plans de sécurité basés sur la méthode MEHARI

PROGRAMME

Jour 1 : Introduction aux concepts et aux étapes de la méthode d'analyse de risque MEHARI

Jour 2 : Conduire une analyse de risque en utilisant la méthode MEHARI

Jour 3 : Planification de la sécurité selon la méthode MEHARI et préparation à l'examen final

DURÉE
3 jours
(21 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

INTRODUCTION À LA GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION CONFORME À LA NORME ISO/IEC 27035

La formation d'introduction à la norme ISO/IEC 27035 vous permettra d'appréhender les concepts fondamentaux de la gestion des incidents de la sécurité de l'information.

En participant à la formation d'introduction ISO/IEC 27035, vous allez comprendre l'importance de la gestion des incidents de sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

Mise à jour : Janvier 2024

F-ISO27035IN

ISO 27035 INTRODUCTION

FORMATION CERTIFIÉE PECB

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par la gestion des incidents de sécurité de l'information et souhaitant acquérir des connaissances relatives aux principaux processus de la gestion des incidents de sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Connaître les concepts, approches, méthodes et techniques permettant de gérer les incidents de sécurité de l'information
- Comprendre les bonnes pratiques de la gestion des incidents de sécurité de l'information

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION

Aucune

PROGRAMME

Jour 1 : Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/IEC 27035

DURÉE
1 jour
(7 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

APPRÉHENDER LES MEILLEURES PRATIQUES RELATIVES À LA GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION SELON L'ISO/IEC 27035

La formation ISO/IEC 27035 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre un plan de gestion des incidents et gérer les incidents de sécurité de l'information. Grâce à cette formation, vous comprendrez les processus de gestion des incidents de sécurité de l'information.

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27035 Foundation ». La certification PECB Foundation atteste que vous avez compris les méthodes fondamentales, les exigences, et l'approche de management.

Mise à jour : Janvier 2024

F-ISO27035FO

ISO 27035 FOUNDATION

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Aucun

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne intéressée par l'approche processus de gestion des incidents de la sécurité de l'information, souhaitant acquérir des connaissances sur les principes et concepts de gestion des incidents de sécurité d'information ou souhaitant poursuivre une carrière dans la gestion des incidents de sécurité de l'information.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre les concepts fondamentaux de la gestion des incidents de sécurité de l'information
- Connaître la corrélation entre la norme ISO/IEC 27035 et les autres normes et cadres règlementaires
- Comprendre l'approche processus permettant de gérer efficacement les incidents de sécurité de l'information

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27035 Foundation* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Concepts et principes fondamentaux de la gestion des incidents de sécurité de l'information
2 : Gestion des incidents de la sécurité de l'information

PROGRAMME

Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/IEC 27035

Jour 2 : Approche processus de gestion des incidents de la sécurité de l'information et préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

MAÎTRISEZ LA GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION SELON LA NORME ISO/IEC 27035

La formation ISO/IEC 27035 Lead Incident Manager vous permettra 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/IEC 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/IEC 27035 prend également en charge l'ISO/IEC 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/IEC 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.

Mise à jour : Janvier 2024

F-ISO27035LM

ISO 27035 LEAD INCIDENT MANAGER

FORMATION CERTIFIÉE PECB

PUBLIC

Gestionnaires des incidents de sécurité de l'information, auditeurs des technologies de l'information, responsables des TIC, souhaitant mettre en place une équipe de réponse aux incidents, souhaitant apprendre davantage sur le fonctionnement efficace d'une équipe de réponse aux incidents, responsables des risques liés à la sécurité de l'information ou responsables de la sécurité de l'information au sein d'une organisation ou administrateurs professionnels des systèmes informatiques et de réseau informatique, membres de l'équipe de réponse aux incidents.

PRÉREQUIS

Une compréhension fondamentale de l'ISO/IEC 27035 et des connaissances approfondies sur la sécurité de l'information. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

OBJECTIFS - APTITUDE - COMPÉTENCES

- 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/IEC 27035**
- Connaître la corrélation entre la norme **ISO/IEC 27035** et les autres normes et cadres réglementaires
- 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
- Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
- Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
- Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

Les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27035 Provisional Incident Manager* ou *Certified ISO/IEC 27035 Incident Manager* ou *Certified ISO/IEC 27035 Lead Incident Manager* ou *Certified ISO/IEC 27035 Senior Lead Incident Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux relatifs à la gestion des incidents liés à la sécurité de l'information

2 : Meilleures pratiques de la gestion des incidents liés à la sécurité de l'information selon la norme ISO/IEC 27035

3 : Conception et développement d'un processus de gestion des incidents organisationnels selon l'ISO/IEC 27035

4 : Préparation aux incidents de sécurité de l'information et mise en œuvre d'un plan de gestion des incidents

5 : Lancement du processus de gestion des incidents et traitement des incidents liés à la sécurité de l'information

6 : Surveillance et mesure de la performance

7 : Améliorer les processus et les activités de gestion des incidents

PROGRAMME

Jour 1 : Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/IEC 27035

Objectifs et structure de la formation, cadres normatifs et réglementaires, gestion des incidents liés à la sécurité de l'information, processus de base de la norme ISO/IEC 27035, principes fondamentaux de la sécurité de l'information, corrélation avec la continuité des activités, questions légales et déontologiques

Jour 2 : Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

Lancement d'un processus de gestion des incidents de sécurité de l'information, compréhension de l'organisation et clarification des objectifs de la gestion des incidents de sécurité de l'information, planifier et préparer, rôles et fonctions, politiques et procédures

Jour 3 : Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information

Planification de la communication, premières étapes de la mise en œuvre, mise en place des éléments de support, détection et rapport, évaluation et décisions, réponses, leçons apprises, transition aux opérations

Jour 4 : Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information

Analyse supplémentaire, analyse des leçons apprises, mesures correctives, compétence et évaluation des gestionnaires d'incidents, clôture de la formation

Jour 5 : Préparation à l'examen final

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

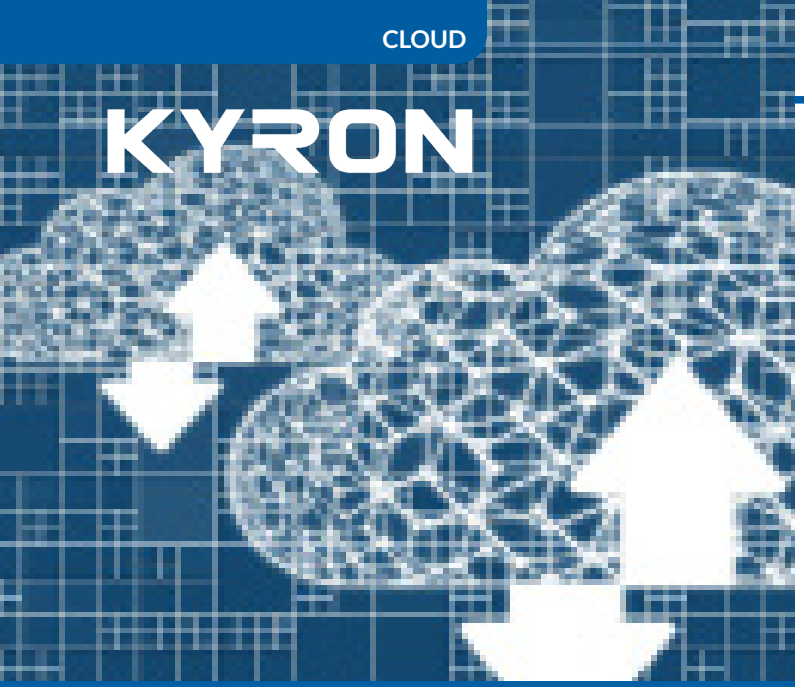
DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON



MAÎTRISER LA MISE EN ŒUVRE ET LA GESTION DU PROGRAMME DE SÉCURITÉ DU CLOUD BASÉ SUR ISO/IEC 27017 ET ISO/IEC 27018

Le nombre croissant d'organismes qui prennent en charge le travail à distance a augmenté l'utilisation des services de cloudcomputing, ce qui a, à son tour, augmenté proportionnellement la demande d'une infrastructure cloud sécurisée.Cette formation est conçue pour aider les participants à acquérir les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud basé sur ISO/IEC 27017 et ISO/IEC 27018. Elle fournit une élaboration complète des concepts et principes du cloud computing, de la gestion des risques de sécurité du cloud computing, des mesures spécifiques au cloud, de la gestion des incidents de sécurité du cloud et des tests de sécurité du cloud.

La formation est suivie de l'examen de certification. Si vous le passez avec succès, vous pouvez demander la certification « PECB Certified Lead Cloud Security Manager ». Un certificat PECB Lead Cloud Security Manager démontre votre capacité et vos compétences à gérer un programme de sécurité du cloud basé sur les meilleures pratiques.

Mise à jour : Janvier 2024

F-CLOUDSECLM

LEAD CLOUD SECURITY MANAGER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

La principale exigence pour participer à cette formation est d'avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018 et une connaissance générale des concepts du cloud computing.
Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne chargée de maintenir et de gérer un programme de sécurité du cloud, professionnels de la sécurité du cloud et de la sécurité de l'information cherchant à gérer un programme de sécurité du cloud, managers ou consultants cherchant à maîtriser les bonnes pratiques de sécurité du cloud, experts techniques cherchant à améliorer leurs connaissances en matière de sécurité du cloud et conseillers experts en sécurité du cloud.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un programme de sécurité du cloud.
- Comprendre la corrélation entre **ISO/IEC 27017, ISO/IEC 27018** et d'autres normes et cadres réglementaires
- Apprendre à interpréter les lignes directrices des normes **ISO/IEC 27017 et ISO/IEC 27018** dans le contexte spécifique d'un organisme
- Développer les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud
- Acquérir les connaissances pratiques pour conseiller un organisme dans la gestion d'un programme de sécurité du cloud en suivant les bonnes pratiques

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified Provisional Cloud Security Manager* ou *Certified Cloud Security Manager* ou *Certified Lead Cloud Security Manager* ou *Certified Senior Lead Cloud Security Manager* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux du cloud computing
2 : Politique de sécurité de l'information pour le cloud computing et la gestion des informations documentées
3 : Gestion des risques de sécurité du cloud computing
4 : Mesures spécifiques au cloud basées sur les normes ISO/IEC 27017 et ISO/IEC 27018 et sur les bonnes pratiques
5 : Sensibilisation, formation, rôles et responsabilités liés à la sécurité du cloud
6 : Gestion des incidents de sécurité du cloud
7 : Tests, surveillance et amélioration continue de la sécurité du cloud

PROGRAMME

Jour 1 : Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et à l'initiation d'un programme de sécurité du cloud
Objectifs et structure de la formation, normes et cadres réglementaires, concepts et principes fondamentaux du cloud computing, comprendre l'architecture du cloud computing de l'organisme, rôles et responsabilités en matière de sécurité de l'information liés au cloud computing, politique de sécurité de l'information pour le cloud computing

Jour 2 : Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud
Gestion des risques de sécurité du cloud computing, sélection et conception de mesures spécifiques au cloud, mise en œuvre de mesures spécifiques au cloud (partie 1)

Jour 3 : Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud
Mise en œuvre de mesures spécifiques au cloud (partie 2), gestion de l'information documentée dans le cloud, sensibilisation et formation à la sécurité du cloud

Jour 4 : Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue
Gestion des incidents de sécurité du cloud, tests de sécurité du cloud, surveillance, mesure, analyse et évaluation, amélioration continue

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

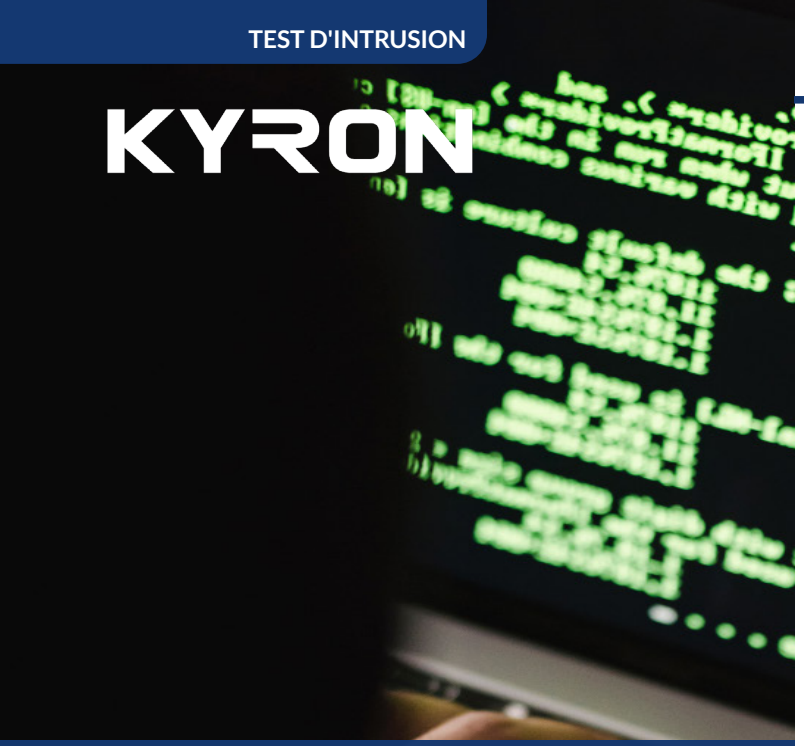
DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON



Le cours Certified Lead Ethical Hacker permet aux participants de développer les compétences et les connaissances nécessaires pour effectuer du piratage éthique, principalement pour les tests d'intrusion des systèmes d'information et des réseaux. Outre des informations théoriques, le cours comprend également des laboratoires qui sont réalisés avec une machine virtuelle.

L'impact des incidents de sécurité dans les petites et grandes organisations a augmenté de manière significative, tout comme la demande de piratage éthique. Le piratage éthique est l'un des outils les plus efficaces pour sauvegarder les actifs et protéger les personnes et les informations. La certification en piratage éthique devient peu à peu une exigence standard pour les professionnels qui veulent travailler dans le domaine de la sécurité de l'information.

La certification PECB Certified Lead Ethical Hacker vous aidera à démontrer votre capacité à évaluer légalement la sécurité des systèmes et à découvrir leurs vulnérabilités.
Comprendre les stratégies des pirates informatiques permet de résoudre les problèmes et les défis en matière de sécurité. Après avoir suivi cette formation, vous serez capable de planifier, de gérer et d'effectuer des tests de pénétration de la sécurité de l'information.

Mise à jour : Janvier 2024

F-ETHICHACK

LEAD ETHICAL HACKER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

La principale condition pour participer à cette formation est d'avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation. Il est recommandé aux participants d'avoir une connaissance des réseaux informatiques et des concepts de programmation.
Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne souhaitant acquérir des connaissances sur les principales techniques utilisées pour effectuer des tests de pénétration. Toute personne impliquée dans la sécurité de l'information qui cherche à maîtriser les techniques de piratage éthique et de tests de pénétration, souhaitant poursuivre une carrière dans le management de la sécurité de l'information. Toute personne responsable de la sécurité des systèmes d'information, telles que les responsables de la sécurité de l'information et les professionnels de la cybersécurité professionnelle. Membres de l'équipe de sécurité de l'information qui cherchent à améliorer leurs connaissances en la matière, managers ou les conseillers experts souhaitant apprendre à gérer les activités de piratage éthique et experts techniques souhaitant apprendre comment planifier et réaliser un test de pénétration.

OBJECTIFS - APTITUDE - COMPÉTENCES

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

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(6h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified Lead Ethical Hacker* via un Voucher qui sera transmis par mail. En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétence**s suivants :

1 : Outils et techniques de collecte d'informations
2 : Modélisation des menaces et identification des vulnérabilités
3 : Techniques d'exploitation
4 : Privilèges
5 : Pivot et transferts de fichiers
6 : Rapports

PROGRAMME

Jour 1 : Introduction au piratage éthique
Objectifs et structure de la formation, normes en matière de tests de pénétration et méthodologie, concepts fondamentaux du piratage éthique, principes de base des réseaux, comprendre la cryptographie, tendances et technologies pertinentes, les fondamentaux de Kali Linux, Initiation du test de pénétration, analyse de la portée des tests de pénétration, implications juridiques et accord contractuel

Jour 2 : Initier la phase de reconnaissance
Reconnaissance passive, reconnaissance active, identification des vulnérabilités

Jour 3 : Lancement de la phase d'exploitation
Modèle de menace et plan d'attaque, éviter les systèmes de détection d'intrusion, attaques au niveau du serveur, attaques côté client, attaques des applications web, attaques WIFI, privilèges, transfert de fichiers, maintien des accès

Jour 4 : Post-exploitation et rapport
Nettoyage et destruction des artefacts, générer un rapport de conclusions, recommandations sur l'atténuation des vulnérabilités identifiées

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

INTRODUCTION AU SYSTÈME DE MANAGEMENT DE LA CONTINUITÉ D'ACTIVITÉ CONFORME À LA NORME ISO 22301

La formation d'introduction à la norme ISO 22301 vous permettra d'appréhender les concepts fondamentaux d'un Système de management de la continuité d'activité.

En participant à la formation d'introduction ISO 22301, vous allez comprendre l'importance d'un Système de management de la continuité d'activité et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO22301IN

ISO 22301 INTRODUCTION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne intéressée par le management de la continuité d'activité ou souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la continuité d'activité.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Connaître les concepts, approches, méthodes et techniques permettant de mettre en œuvre un Système de management de la continuité d'activité
- Comprendre les éléments fondamentaux d'un Système de management de la continuité d'activité

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION

Aucune

PROGRAMME

Jour 1 : Concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO /IEC 27001

DURÉE
1 jour
(7 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

APPRÉHENDER LES MEILLEURES PRATIQUES EN MATIÈRE DE SYSTÈMES DE MANAGEMENT DE LA CONTINUITÉ D'ACTIVITÉ CONFORMES À L'ISO 22301

Cette formation est conçue pour aider les participants à comprendre les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301. En participant à cette formation, les participants en apprendront davantage sur la structure et les exigences de la norme, notamment la politique du SMCA, l'engagement de la direction générale, l'audit interne, la revue de direction et le processus d'amélioration continue.

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et, si vous le réussissez, vous pouvez faire une demande de certification « PECB Certified ISO 22301 Foundation ». Un certificat Foundation de PECB montre que vous avez des connaissances sur les concepts fondamentaux, les principes, les méthodologies, les exigences, le cadre et l'approche de management utilisés dans la continuité d'activité.

Mise à jour : Janvier 2024

FORMATION CERTIFIÉE PECB

F-ISO22301FO

ISO 22301 FOUNDATION

PRÉREQUIS
Aucun

DÉLAI ET MOYEN D'ACCÈS
- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES
- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC
Toute personne impliquée dans le management de la continuité d'activité, souhaitant acquérir des connaissances relatives aux principaux processus d'un système de management de la continuité d'activité ou souhaitant poursuivre une carrière dans le management de la continuité d'activité.

OBJECTIFS - APTITUDE - COMPÉTENCES
- Comprendre les éléments et le fonctionnement d'un Système de management de la continuité d'activité et ses principaux processus
- Comprendre la corrélation entre la norme **ISO 22301** et les autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management de la continuité d'activité

APPROCHE PÉDAGOGIQUE
- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national Qualité des organismes de formation.

CERTIFICATION *(1h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO 22301 Foundation* via un Voucher qui sera transmis par mail.

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :
1 : Principes et concepts fondamentaux du système de management de la continuité d'activité (SMCA)
2 : Système de management de la continuité d'activité (SMCA)

PROGRAMME

Jour 1 : Introduction au système de management de la continuité d'activité (SMCA) et à ISO 22301

Jour 2 : Système de management de la continuité d'activité et préparation à l'examen de certification

DURÉE
2 jours
(14 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

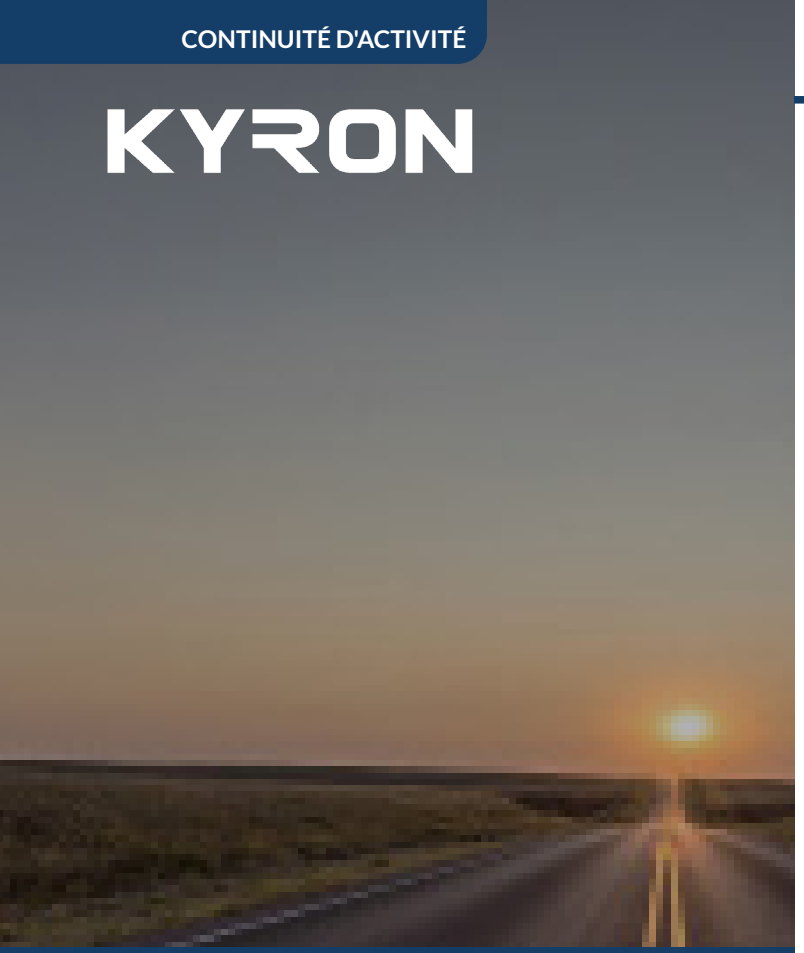
DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON



La formation ISO 22301 Lead Implementer vous permettra 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.

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la continuité d'activité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 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 22301 dans une organisation.

Mise à jour : Janvier 2024

F-ISO22301LI

ISO 22301 LEAD IMPLEMENTER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de sa mise en œuvre. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

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 et membres d'une équipe du SMCA.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre la corrélation entre la norme **ISO 22301** et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA
- Savoir interpréter les exigences de la norme **ISO 22301** dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du **SMCA**
- 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

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO 22301 Provisional Implémenter* ou *Certified ISO 22301 Implementer* ou *Certified ISO 22301 Lead Implémenter* ou *Certified ISO 22301 Master* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux de la continuité d'activité
2 : Exigences relatives au système de management de la continuité d'activité (SMCA)
3 : Planification d'une mise en œuvre du SMCA basée sur ISO 22301
4 : Mise en œuvre d'un SMCA basé sur ISO 22301
5 : Evaluation de la performance et suivi et mesure d'un SMCA basé sur ISO 22301
6 : Amélioration continue d'un SMCA basé sur ISO 22301
7 : Préparation à un audit de certification SMCA

PROGRAMME

Jour 1 : Introduction à l'ISO 22301 et déclenchement d'un SMCA
Objectifs et structure de la formation, normes des systèmes de management, principes et concepts fondamentaux de la continuité d'activité, système de management de la continuité d'activité, déclenchement de la mise en œuvre du SMCA, compréhension de l'organisme et de son contexte, analyse du système existant, périmètre du SMCA

Jour 2 : Plan de mise en œuvre d'un SMCA
Leadership et engagement, stratégies et solutions de continuité d'activité, plans et procédures de continuité d'activité, plan d'intervention en cas d'incident, plan d'intervention d'urgence, plan de gestion de crise, communication

Jour 3 : Mise en œuvre d'un SMCA
Évaluation des risques, stratégies et solutions de continuité d'activité, plans et procédures de continuité d'activité, plan d'intervention en cas d'incident, plan d'intervention d'urgence, plan de gestion de crise, communication

Jour 4 : Suivi du SMCA, amélioration continue et préparation à l'audit de certification
Programmes d'exercices, surveillance, mesure, analyse et évaluation, audit interne, revue de direction, traitement des non-conformités, amélioration continue, préparation à l'audit de certification, processus de certification et clôture de la formation

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISEZ L'AUDIT D'UN SYSTÈME DE MANAGEMENT DE LA CONTINUITÉ D'ACTIVITÉ CONFORME À LA NORME ISO 22301

Étant donné le nombre croissant de perturbations et l'imprévisibilité des catastrophes de toutes sortes (naturelles, professionnelles, sécurité de l'information), les organismes visent aujourd'hui à obtenir la certification ISO 22301 afin de montrer leur engagement envers la continuité d'activité et de garantir que les incidents perturbateurs sont détectés et traités correctement, ce qui permet d'améliorer continuellement le système de management. En devenant un auditeur certifié PECB, vous recevrez une reconnaissance formelle et indépendante de votre compétence personnelle et vous pourrez réaliser des audits SMCA pour un organisme de certification.

PECB a conçu la formation d'auditeur principal ISO 22301, en reconnaissant l'importance d'un audit efficace et les moyens utilisés pour le mener à bien. En participant à cette formation, vous acquérez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément à la norme ISO 19011 et le processus de certification selon la norme ISO/IEC 17021-1.

Grâce à des sessions interactives, des informations explicatives, des exercices et des questions à discuter, vous pourrez acquérir des connaissances sur le système de management de la continuité d'activité ainsi que sur les techniques d'audit et devenir compétent pour réaliser un audit du SMCA en appliquant des principes, des procédures et des techniques d'audit largement reconnus, et pour gérer un programme d'audit et une équipe d'audit.

Après avoir suivi la formation, vous pouvez vous présenter à l'examen et, si vous le réussissez, vous pouvez demander la certification « PECB Certified ISO 22301 Lead Auditor ». Le certificat internationalement reconnu « PECB Certified ISO 22301 Lead Auditor » prouvera que vous avez les capacités et les compétences professionnelles pour auditer des organismes sur la base des exigences d'ISO 22301 et des bonnes pratiques d'audit.

Mise à jour : Janvier 2024

F-ISO22301LA

ISO 22301 LEAD AUDITOR

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit. Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

PUBLIC

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, toute personne responsable du maintien de la conformité aux exigences du SMCA, experts techniques désirant préparer un audit du système de management de la continuité d'activité et conseillers spécialisés en management de la continuité d'activité.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Comprendre le fonctionnement d'un Système de management de la continuité d'activité **(SMCA)** conforme à la norme **ISO 22301**
- Expliquer la corrélation entre la norme **ISO 22301** et les autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme **ISO 19011**
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'**ISO 22301** dans le contexte d'un audit du **SMCA**
- 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**

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO 22301 Provisional Auditor* ou *Certified ISO 22301 Auditor* ou *Certified ISO 22301 Lead Auditor* ou *Certified ISO 22301 Senior Lead Auditor* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies).

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires. Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux du système de management de la continuité d'activité (SMCA)
2 : Système de management de la continuité d'activité (SMCA)
3 : Concepts et principes fondamentaux de l'audit
4 : Préparation d'un audit ISO 22301
5 : Réalisation d'un audit ISO 22301
6 : Clôture d'un audit ISO 22301
7 : Gestion d'un programme d'audit ISO 22301

PROGRAMME

Jour 1 : Introduction au système de management de la continuité d'activité (SMCA) et à ISO 22301
Objectifs et structure de la formation, normes et cadres réglementaires, processus de certification, principes fondamentaux de la continuité d'activité, système de management de la continuité d'activité (SMCA)

Jour 2 : Principes d'audit, préparation et initiation d'un audit
Concepts et principes fondamentaux de l'audit, impact des tendances et de la technologie dans le domaine de l'audit, audit basé sur des preuves, audit basé sur des risques, faisabilité de l'audit, audit de l'étape 1

Jour 3 : Activités d'audit sur site
Préparation de l'audit de l'étape 2 (audit sur site), audit de l'étape 2, communication durant l'audit, procédures d'audit, création de plans de test d'audit

Jour 4 : Clôture de l'audit
Rédaction des conclusions d'audit et des rapports de non-conformité, documentation d'audit et examen de la qualité, clôture de l'audit, évaluation des plans d'action par l'auditeur, après l'audit initial, gestion d'un programme d'audit interne

Jour 5 : Préparation à l'examen de certification

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

MAÎTRISER LA MISE EN ŒUVRE ET LE MANAGEMENTDUSYSTÈMEDEMANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE (PIMS) SELON LA NORME ISO/IEC 27701

La formation ISO/IEC 27701 Lead Implementer vous permet de développer l'expertise nécessaire pour aider une organisation à établir, mettre en œuvre, entretenir et améliorer continuellement un système de management de la protection de la vie privée basé sur ISO/IEC 27701 en améliorant un système de management de la sécurité de l'information (SMSI) existant basé sur la norme ISO/IEC 27001 et les directives d'ISO/IEC 27002.

Cette formation est conçue pour préparer les participants à mettre en œuvre un système de management de la protection de la vie privée (Privacy Information Management System – PIMS) conformément aux exigences et aux directives de la norme ISO/IEC 27701. De plus, vous obtiendrez une compréhension globale des meilleures pratiques de management de la protection de la vie privée et apprendrez comment gérer et traiter les données tout en respectant les diverses lois de protection de la vie privée.

Après avoir maîtrisé la mise en œuvre et le management d'un système de management de la protection de la vie privée, vous pouvez passer l'examen et demander une certification PECB Certified ISO/IEC 27701 Lead Implementer. La certification PECB Lead Implementer, reconnue internationalement, prouve que vous disposez des connaissances pratiques et des capacités professionnelles pour mettre en œuvre les exigences d'ISO/IEC 27701 dans une organisation.

Mise à jour : Janvier 2024

F-ISO27701LI

ISO 27701 LEAD IMPLEMENTER

FORMATION CERTIFIÉE PECB

PRÉREQUIS

Compréhension fondamentale de la sécurité de l'information et connaissance approfondie des principes de mise en œuvre du SMSI.
Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Superviseurs et consultants impliqués dans la confidentialité et la gestion des données, experts-conseils cherchant à maîtriser la mise en œuvre d'un système de management de la protection de la vie privée, membres de l'équipe PIMS, responsables des informations personnellement identifiables (IPI) au sein des organisations et responsables de la conformité aux exigences des lois de protection des données.

OBJECTIFS - APTITUDE - COMPÉTENCES

- Maîtriser les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS
- En savoir plus sur la corrélation entre **ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002** et d'autres normes et cadres réglementaires
- Comprendre le fonctionnement d'un PIMS basé sur **ISO/IEC 27701** et ses processus principaux
- Apprendre à interpréter les exigences d'**ISO/IEC 701** dans le contexte spécifique d'une organisation
- Développer l'expertise nécessaire pour aider une organisation à planifier, mettre en œuvre, gérer, surveiller et gérer efficacement un PIMS

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27701 Provisional Implémenter* ou *Certified ISO/IEC 27701 Implémenter* ou *Certified ISO/IEC 27701 Lead Implémenter* ou *Certified ISO/IEC 27701 Senior Lead Implémenter* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux d'un système de management de la protection de la vie privée (PIMS)
2 : Mesures de bonnes pratiques du système de management de la protection de la vie privée
3 : Planification de la mise en œuvre du PIMS selon ISO/IEC 27701
4 : Mise en œuvre d'un PIMS conforme à ISO/IEC 27701
5 : Evaluation de performance, surveillance et mesure d'un PIMS selon ISO/IEC 27701
6 : Amélioration continue d'un PIMS selon ISO/IEC 27701
7 : Préparation à un audit de certification du PIMS

PROGRAMME

Jour 1 : Introduction à l'ISO 27701 et initiation au PIMS
Objectifs et structure de la formation, normes et cadres réglementaires, système de management de la protection de la vie privée (IMS), concepts et principes fondamentaux de la sécurité de l'information et de la protection de la vie privée, démarrage de la mise en œuvre du PIMS, analyse de domaine de l'application du SMSI et de la déclaration d'applicabilité, domaine d'application du PIMS, approbation de la direction, politique de protection de la vie privée, appréciation du risque d'atteinte à la vie privée.

Jour 2 : Planification de la mise en œuvre d'un PIMS
Appréciation de l'impact sur la vie privée, déclaration d'applicabilité du PIMS, gestion de la documentation, sélection des mesures, mise en œuvre des mesures

Jour 3 : Mise en œuvre d'un PIMS
Mise en œuvre des mesures (suite), mise en œuvre des mesures spécifiques aux contrôleurs IPI, mise en œuvre des mesures spécifiques aux processeurs IPI

Jour 4 : Surveillance du PIMS, amélioration continue et préparation d'un audit de certification
Sensibilisation, formation et communication, surveillance, mesure, analyse, évaluation et revue de direction, audit interne, traitement des non-conformités, amélioration continue, préparation à l'audit de certification, processus de certification

Jour 5 : Préparation à l'examen de certification

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

F-ISO27701LA

ISO 27701 LEAD AUDITOR

FORMATION CERTIFIÉE PECB

MAÎTRISER L'AUDIT DU SYSTÈME DE MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE (PIMS) BASÉ SUR LA NORME ISO/IEC 27701

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 27701 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.

Mise à jour : Janvier 2024

PRÉREQUIS

Une compréhension fondamentale de la sécurité de l'information et de la protection de la vie privée, et une connaissance approfondie des principes d'audit.
Pour s'assurer des connaissances de base, un test QCM sera réalisé avant le début de la formation.

DÉLAI ET MOYEN D'ACCÈS

- Un entretien de positionnement est effectué en amont pour proposer une formation adaptée répondant à vos besoins et attentes. Une proposition tarifaire vous sera adressée en suivant par mail.
- À compter de la signature du devis, le délai moyen pour débuter la formation est de 45 jours.

MOYENS PÉDAGOGIQUES

- Les stagiaires accèdent à leur manuel au format électronique, exposant les sujets traités, les exercices et ateliers ; ainsi que différents liens renvoyant à des ressources ayant rapport avec le cours, des lectures complémentaires et les réponses aux questions des ateliers.
- Dans le cadre d'une formation en présentiel, les supports de cours sont projetés à l'aide d'un vidéo-projecteur.
- Dans le cadre d'une formation en distanciel, une visio-conférence est effectuée à l'aide du logiciel Teams ou Zoom avec partage en ligne des supports de cours.
- Mise en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif.

PUBLIC

Toute personne responsable du maintien de la conformité aux exigences du PIMS, auditeurs cherchant à réaliser et à diriger des audits de certification du système de management de la protection de la vie privée (PIMS), gestionnaires ou consultants souhaitant maîtriser un processus d'audit du PIMS, experts techniques souhaitant se préparer à un audit du PIMS et experts-conseils en matière de protection des informations d'identification personnelle (IIP).

OBJECTIFS - APTITUDE - COMPÉTENCES

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

APPROCHE PÉDAGOGIQUE

- Les cours de formation 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

MODALITÉS DE SUIVI

- Les modalités de suivi ont pour but de s'assurer de la présence de l'apprenant.
- Dans le cadre de formations en présentiel, les feuilles de présence sont émargées à la demi-journée (3h30). Ces dernières justifient que le stagiaire était présent pendant toute la durée de la formation.
- Pour les formations à distance, le suivi est effectué à partir des dates, heures et durées de connexion des stagiaires à la plateforme de formation.

MODALITÉS D'ÉVALUATION

- Les modalités d'évaluation ont pour but de s'assurer de l'intégration et de l'assimilation des apprenants tout au long de la formation.
- Elles sont effectuées à partir des feuilles d'évaluations : des acquis des connaissances, de l'amélioration des compétences et/ou des ancrages professionnels visés.
- Des évaluations sont effectuées pour cela en amont de la formation, durant la formation et post formation.
- Une évaluation des acquis finale sera effectuée à la fin de la formation pour s'assurer que les objectifs pédagogiques ont été atteints.

DURÉE
5 jours
(35 heures)

PRIX
Nous consulter
Min 5 personnes

DATES
Consulter le calendrier

REPAS
Inclus

PRÉSENTIEL
KYRON
ou site client

DISTANCIEL
Nous consulter

ÉVALUATION DE LA SATISFACTION DU PARTICIPANT À LA FORMATION

Le processus d'évaluation a pour objectif de déterminer la satisfaction du stagiaire quant à la prestation et aux conditions de déroulement de la formation, l'atteinte des objectifs pédagogiques, l'atteinte des objectifs de formation, la pertinence de l'action de formation et si le stagiaire a acquis ou amélioré les compétences dont l'objectif principal a été défini par l'action de formation.

INTERVENANTS

KYRON est entourée d'une équipe de formateurs expérimentés et détenteurs des certifications proposées respectant la démarche du référentiel national qualité des organismes de formation.

CERTIFICATION *(3h d'examen)*

A la fin de la formation, les participants peuvent s'inscrire à l'examen de certification *Certified ISO/IEC 27701 Provisional Auditor* ou *Certified ISO/IEC 27701 Auditor* ou *Certified ISO/IEC 27701 Lead Auditor* ou *Certified ISO/IEC 27701 Senior Lead Auditor* (selon les exigences relatives à la qualification sélectionnée) via un Voucher qui sera transmis par mail (voir https://pecb.com/fr/certification-rules-and-policies). Le prix de la certification est inclus dans le prix de la formation.

L'examen couvre les **domaines de compétences** suivants :

1 : Principes et concepts fondamentaux d'un système de management de la protection de la vie privée (PIMS)
2 : Exigences du système de management de la protection de la vie privée (PIMS)
3 : Concepts et principes fondamentaux de l'audit
4 : Préparation d'un audit ISO/IEC 27701
5 : Réalisation d'un audit ISO/IEC 27701
6 : Clôture d'un audit ISO/IEC 27701
7 : Gestion d'un programme d'audit ISO/IEC 27701

PROGRAMME

Jour 1 : Introduction au système de management de la protection de la vie privée (PIMS) et à la norme ISO/IEC 27701
Objectifs et structure de la formation, normes et cadres réglementaires, processus de certification, principes et concepts fondamentaux en matière de sécurité de l'information et de protection de la vie privée, système de management de la protection de la vie privée (PIMS)

Jour 2 : Principes d'audit, préparation et ouverture d'un audit
Concepts et principes fondamentaux de l'audit, Impact des tendances et de la technologie sur l'audit, audit basé sur des preuves, audit basé sur les risques, Initiation du processus d'audit, étape 1 de l'audit

Jour 3 : Activités d'audit sur site
Préparation de l'étape 2 de l'audit (audit sur site), étape 2 de l'audit, communication pendant l'audit, procédures d'audit, création de plans de test d'audit

Jour 4 : Clôture de l'audit
Rédaction des constatations d'audit et des rapports de non-conformité, documentation d'audit et revue de qualité, clôture de l'audit, évaluation des plans d'action par l'auditeur, au-delà de l'audit initial, gestion d'un programme d'audit interne, clôture de la formation

Jour 5 : Préparation à l'examen de certification

ACCÉSSIBILITÉ

En cas de situation de handicap, une étude sera effectuée pour proposer une formation et des aménagements adaptés. Une salle de formation répondant aux normes d'accessibilité et d'accueil du public sera mise à disposition.
Contactez-nous : training@kyron.fr.

-Support en français, formation dispensée en français-

KYRON

KYRON

Your Cyber our Concern

training@kyron.fr
+33 (0)5 34 47 86 65
www.kyron.fr