

Élaborer et mettre en oeuvre une démarche de cybersécurité (27001 Lead Implementer)

Formation Management / Référentiels et Méthodes / Global Best Practice



Cette formation de 5 jours vise à réussir la certification "Élaborer et mettre en oeuvre une démarche de cybersécurité" en Français (Certificateur : ESIC). Par ailleurs, le contenu de cette formation permet également de couvrir tous les objectifs de la certification 27001 Lead Implementer de PECB.

OBJECTIFS

- Piloter la gouvernance de la cybersécurité
- Gérer des systèmes d'information sécurisés
- Gérer les risques et protection des systèmes
- Évaluer le niveau de sécurité
- Gestion des incidents de cybersécurité

PUBLIC

Toute personne désireuse de réussir la certification Élaborer et mettre en oeuvre une démarche de cybersécurité (27001 Lead Implementer)

PRE-REQUIS

Il n'y a pas de Pré-requis pour suivre cette formation Élaborer et mettre en oeuvre une démarche de cybersécurité (27001 Lead Implementer).

PROGRAMME

Pilotage de la gouvernance de la cybersécurité

Définir les orientations de cybersécurité
Définir les moyens alloués à la cybersécurité
Établir une cartographie fonctionnelle
Définir l'organisation et les responsabilités en matière de cybersécurité
Établir la documentation de cybersécurité
Intégrer la cybersécurité dans les projets
Définir et utiliser des indicateurs cybersécurité
Communiquer en interne et sensibiliser le personnel

Gestion des systèmes d'information sécurisés

Cartographier les systèmes
Sécuriser la manipulation des informations sensibles
Concevoir et développer des systèmes sûrs
Gérer les chaînes d'approvisionnement
Valider la cybersécurité lors de la recette
Exploiter de manière sécurisée
Gérer la maintenance et le maintien en condition de sécurité
Encadrer l'évolution des systèmes

Gestion des risques et protection des systèmes

Analyser les risques cyber relatifs aux systèmes
Homologuer les systèmes d'information
Confirmer le développement de confiance des composants
Utiliser des composants qualifiés
Configurer correctement ses composants
Utiliser des services cryptographiques à l'état de l'art et protéger ses clés
Garantir la robustesse des authentifiants et mots de passe
Garantir la disponibilité des servitudes

Évaluation du niveau de sécurité

Identifier les écarts au référentiel
Évaluer par rapport à l'état de l'art
Rechercher des traces de compromission
Corriger les problèmes identifiés
Organiser des entraînements et des exercices à destination du personnel afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles
Organiser des entraînements et des exercices à destination des prestataires externes afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles

Gestion des incidents de cybersécurité

Disposer d'une chaîne opérationnelle de gestion des incidents

A retenir

Durée : **5 jours** soit 35h.
Réf. **IS27001LI-CPF**
Code CPF : **1**

Cette formation Référentiels et Méthodes prépare à une **Certification officielle.**

L'examen CERTyou est passé après la formation.

01 42 93 52 72

Dates des sessions

Paris
05/12/2022
Lille
28/11/2022

Cette formation est également proposée en formule **INTRA-ENTREPRISE.**



Inclus dans cette formation



EXAMEN CERTyou COMPRIS DANS LE TARIF

Pour toutes nos formations certifiantes, nous incluons les frais de certification dans le tarif de la formation. Comparez bien les offres de formation du marché : notre offre étant la plus complète, vous serez alors plus serein dans la préparation de vos certifications.

CERTYOU, 37 rue des Mathurins, 75008 PARIS

Tél : +33 1 42 93 52 72 - contact@certyou.com - www.certyou.com

RCS de Paris n° 804 509 461 - TVA intracommunautaire FR03 804509461 - APE 8559A

Déclaration d'activité enregistrée sous le N° 11 75 52524 75 auprès du préfet de région d'Ile-de-France

Élaborer et mettre en oeuvre une démarche de cybersécurité (27001 Lead Implementer)

Formation Management / Référentiels et Méthodes / Global Best Practice



Collecter les événements de sécurité
Détecter les événements anormaux
Reconstituer le scénario des incidents, les vecteurs et leur étendue
Évaluer l'impact et le périmètre de l'incident sur l'activité
Organiser la réaction
Préparer des mesures de réaction
Conduire la réaction

Horaires, Planning et Déroulement de cette formation

Horaires

- Formation de 9h00 (9h30 le premier jour) à 17h30.
- Deux pauses de 15 minutes le matin et l'après-midi.
- 1 heure de pause déjeuner

DEROULEMENT

- Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
- Une attestation de suivi de formation vous sera remise en fin de formation.
- Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

[Réussir la Certification Gestion de Projet PMP du PMI](#)

[Réussir la Certification PRINCE2 Foundation](#)

[Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner](#)

[Réussir la Certification ITIL Foundation](#)

[Réussir la Certification Agile certifié SCRUM Master](#)

[Réussir les Certifications TOGAF Certified et TOGAF Foundation](#)

CERTyou est certifié Qualiopi

CERTyou a été reconnu par le BUREAU VERITAS pour la qualité de ces procédures et lui a décerné la certification Qualiopi Formation Professionnelle. La certification de services Qualiopi Formation Professionnelle répond aux exigences qualité décrites dans l'article 1 du décret n°2015-790 du 30 juin 2015.



La certification qualité a été délivrée au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

Retrouvez cette formation sur notre site :

[Élaborer et mettre en oeuvre une démarche de cybersécurité \(27001 Lead Implementer\)](#)



Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100%
SATISFACTION
GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.